MOXA EtherDevice™ Switch User's Manual

EDS-508 Series

www.moxa.com/product

Second Edition, November 2004

Moxa Networking Co., Ltd.
Tel: +886-2-2910-1230
Fax: +886-2-2910-1231
Web: www.moxa.com

MOXA Technical Support
Worldwide: support@moxanet.tw
The Americas support@moxa.com

MOXA EtherDevice™ Switch (EDS)
User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2004 Moxa Networking Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA is a registered trademark of the Moxa Group.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Table of Contents

Chapter 1 Introduction 1-1

Inside the Future of Industrial Ethernet Technology 1-2
- The trend in industrial communications and automation applications 1-2
- Industrial vs. Commercial 1-2
- Informative vs. Passive 1-2

MOXA EtherDevice™ Switch 1-2
Package Checklist 1-2
Features 1-3
- Advanced Industrial Networking Capability 1-3
- Designed for Industrial Applications 1-3
- Useful Utility and Remote Configuration 1-3

Chapter 2 Getting Started 2-1

Using the RS-232 Serial Console (115200, None, 8, 1, VT100) 2-2
Using the Telnet Console 2-4
Using Web Configuration 2-6

Chapter 3 Featured Functions 3-1

Configuring Basic Settings 3-2
- System Identification 3-2
- Password 3-3
- Accessible IP 3-4
- Port 3-5
- Network 3-7
- Time 3-8
- System File Update—By Remote TFTP 3-10
- System File Update—By Local Import/Export 3-11
- Factory Default 3-12

Using Port Trunking 3-12
- The Concept of Port Trunking 3-12

Configuring Port Trunking 3-13
- Port Trunking Settings 3-13
- Port setting information 3-14

Using SNMP 3-14
- Configuring SNMP 3-15
- SNMP Read/Write Settings 3-15
- Private MIB information 3-17

Using Communication Redundancy 3-17
- The Concept of Turbo Ring 3-17
- Configuring Turbo Ring 3-21
- The Concept of STP/RSTP 3-22
- Configuring STP/RSTP 3-27

Using Traffic Prioritization 3-30
- The Concept of Traffic Prioritization 3-30
- Configuring Traffic Prioritization 3-32

Using Virtual LAN 3-35
- The Concept of Virtual LAN (VLAN) 3-35

Sample Applications of VLANs using MOXA EtherDevice Switch 3-37
Configuring 802.1Q VLAN 3-38
Using Multicast Filtering 3-40
The Concept of Multicast Filtering 3-40
Configuring Multicast Filtering 3-42
Add Static Multicast MAC 3-44
Using Rate Limiting 3-44
Configuring Rate Limiting 3-45
Using Port Lock 3-46
Adding a Static Unicast MAC Address 3-46
Configuring Port Lock 3-47
Using Auto Warning 3-47
Configuring Email Warning 3-47
Email Alarm Events Settings 3-48
Email Settings 3-49
Configuring Relay Warning 3-50
Relay Alarm Events Settings 3-51
Relay Alarm List 3-52
Using Line-Swap-Fast-Recovery 3-52
Configuring Line-Swap Fast Recovery 3-53
Using Set Device IP 3-53
Configuring Set Device IP 3-54
Using Diagnosis 3-55
Mirror Port 3-55
Ping 3-56
Using Monitor 3-56
Monitor by Switch 3-56
Monitor by Port 3-57
Using the MAC Address Table 3-58
Using Event Log 3-59

Chapter 4 EDS Configurator GUI 4-1
Starting EDS Configurator 4-2
Broadcast Search 4-2
Search by IP address 4-3
Upgrade Firmware 4-4
Modify IP Address 4-4
Export Configuration 4-5
Import Configuration 4-6
Unlock Server 4-7

Appendix A MIB Groups A-1

Appendix B Specifications B-1

Appendix C Service Information C-1
MOXA Internet Services C-2
Problem Report Form C-3
Product Return Procedure C-4

1

Introduction

Welcome to MOXA EtherDevice Switch EDS-508 Series, the world's first intelligent Ethernet Device Switch specially designed for connecting Ethernet-enabled devices in industrial field applications.

The following topics are covered in this chapter:

- **Inside the Future of Industrial Ethernet Technology**
- **MOXA EtherDevice™ Switch**
- **Package Checklist**
- **Features**

Inside the Future of Industrial Ethernet Technology

The trend in industrial communications and automation applications

As the world's network and information technology becomes more mature, the trend is to use Ethernet as the major communications interface in many industrial communications and automation applications. In fact, a whole new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

Industrial vs. Commercial

Users have found that when moving Ethernet from the comfortable office environment to the harsh and less predictable industrial environment, the commercial Ethernet equipment available in today's market simply cannot meet the high reliability requirements demanded by industrial applications. This means that a more robust type of network equipment, commonly referred to as *industrial* Ethernet equipment, is required for these applications.

Informative vs. Passive

Since industrial Ethernet devices are often located at the endpoints of a system, such devices cannot always know what's happening elsewhere on the network. This means that industrial Ethernet communication equipment that connects these devices must take responsibility for providing system maintainers with real-time alarm messages.

MOXA EtherDevice™ Switch

MOXA EtherDevice Switch comes with a suite of useful maintenance and monitoring functions, and is designed to provide smooth and reliable operation in harsh industrial environments. You will find that MOXA EtherDevice Switch establishes a new industrial Ethernet benchmark. It is excellent for keeping automation systems running continuously, is ideal for sending status reports to help prevent system damages and losses, is a great tool for mastering your industrial Ethernet networks, and is well-suited for use with industrial device control networks.

ATTENTION

Throughout this User's Manual, we often use EDS as an abbreviation for MOXA EtherDevice Switch:

EDS = MOXA EtherDevice Switch

Package Checklist

MOXA EtherDevice Switch EDS-508 Series is shipped with the following items:

- 1 MOXA EtherDevice Switch EDS-508
- Hardware Installation Guide
- CD-ROM with User's Manual and Windows Utility
- Moxa Product Warranty
- RJ45 to DB9 Console port cable
- Protective caps for unused ports
- Panel mounting kit (Optional ordering)

NOTE: *Notify your sales representative if any of the above items is missing or damaged.*

Features

Advanced Industrial Networking Capability

- MOXA Turbo Ring with Redundant Self-Healing Ethernet Ring Capability (recovery time < 300 ms at full load)
- IGMP Snooping for filtering multicast traffic from industrial Ethernet Protocols
- Supports IEEE 802.1Q VLAN and GVRP protocol to ease network planning
- Supports QoS—IEEE 802.1p/1Q and TOS/DiffServ to increase determinism
- Port Trunking to quadruple bandwidth or provide redundant path

Designed for Industrial Applications

- Long-haul transmit distance of 40 km or 80 km
- -40 to 75°C operating temperature range (for "–T" models)
- Redundant, dual DC power inputs
- IP 30, rugged high-strength case
- DIN-Rail or panel mounting ability
- Rate limiting to prevent unpredictable network status
- Lock port for authorized MAC address access only
- Port mirroring for online debugging
- Automatic warning by exception through email, relay output
- Digital inputs to integrate a sensor and alarm with an IP network
- Automatic recovery of connected device IP addresses
- Line-swap fast recovery (patent pending)

Useful Utility and Remote Configuration

- Web browser, Telnet/Serial console, Windows utility configurable
- Send ping commands to identify network segment integrity

2

Getting Started

This chapter explains how to access MOXA EtherDevice Switch for the first time. There are three ways to access the switch: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect MOXA EtherDevice Switch to a PC's COM port, can be used if you do not know MOXA EtherDevice Switch's IP address. The Telnet console and web browser connection methods can be used to access MOXA EtherDevice Switch over an Ethernet LAN, or over the Internet.

The following topics are covered:

- **Using the RS-232 Serial Console (115200, None, 8, 1, VT100)**
- **Using the Telnet Console**
- **Using Web Configuration**

Using the RS-232 Serial Console (115200, None, 8, 1, VT100)

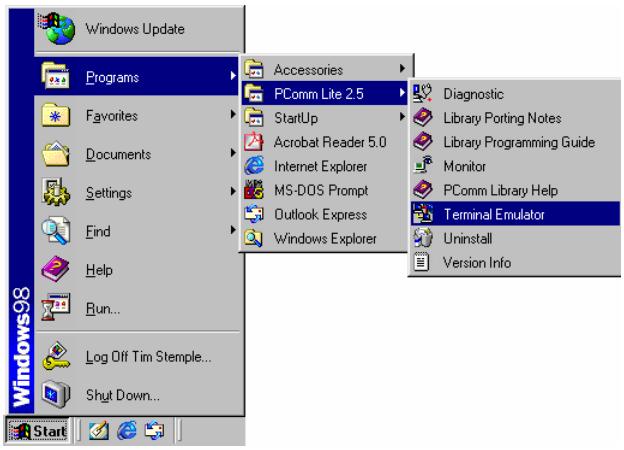
NOTE **Connection Caution!**

1. You **cannot** connect to EDS simultaneously through the serial console and via Telnet.
2. You **can** connect to EDS simultaneously by web browser and serial console, or by web browser and via Telnet.
3. However, we recommend that when connecting to EDS by web browser, you do not simultaneously connect by either serial console or via Telnet.
   By following this advice, you can maintain better control over how your MOXA EtherDevice Switch is managed.

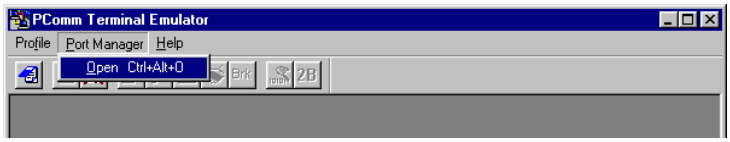
NOTE We recommend using MOXA PComm Terminal Emulator, which can be downloaded free of charge from Moxa's website. After installing PComm Terminal Emulator, take the following steps to access the RS-232 Console utility.

NOTE Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect MOXA EtherDevice Switch's RS-232 Console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

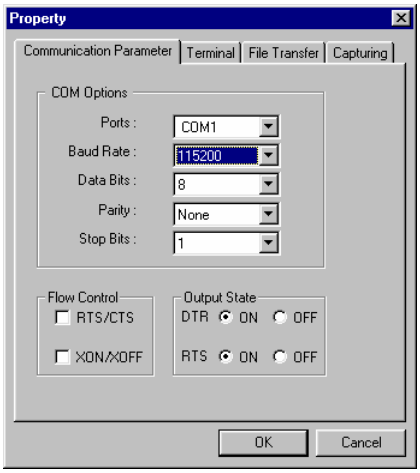
1. From the Windows desktop, click on **Start → Programs → PCommLite2.5 → Terminal Emulator.**



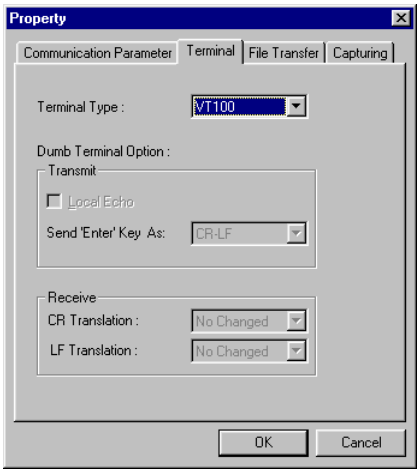
2. Select **Open** under **Port Manager** to open a new connection.



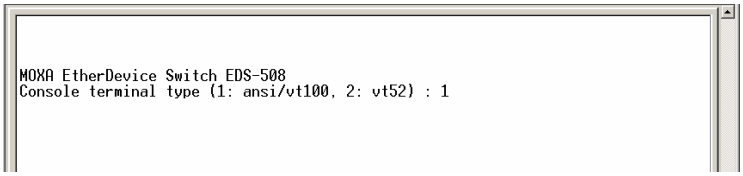
3. The **Communication Parameter** page of the **Property** window opens. Select the appropriate COM port for **Console Connection**, **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



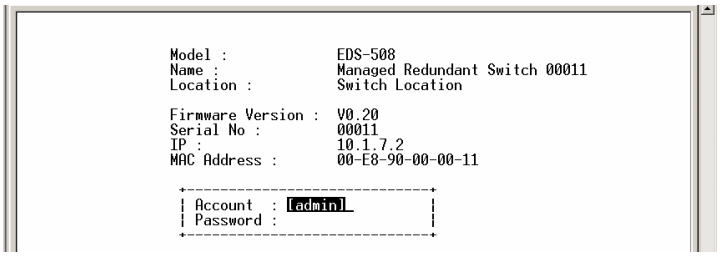
4. Click on the **Terminal** tab, and select **VT100** for **Terminal Type**. Clcik **OK** to confirm.



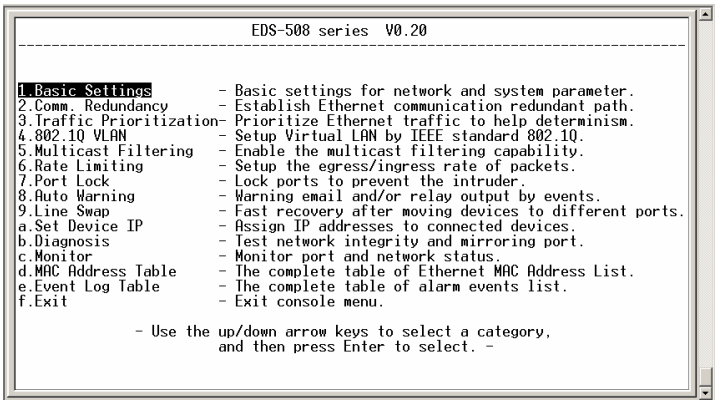
5. Type **1** to select **ansi/VT100** terminal type, and then press **Enter**.



6. If a password has been set for this device, the Console login screen will appear. Enter the **Console Password** (this is the same as the Web Browser password), and then press **Enter**.



7. MOXA EtherDevice Switch's **Main Menu** will be displayed. (To modify the appearance of the PComm Terminal Emulator window, select **Font…** under the **Edit** menu, and then choose the desired formatting options.)


EDS-508 series V0.20
1.Basic Settings - Basic settings for network and system parameter.
2.Comm. Redundancy - Establish Ethernet communication redundant path.
3.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
4.802.1Q VLAN - Setup Virtual LAN by IEEE standard 802.1Q.
5.Multicast Filtering - Enable the multicast filtering capability.
6.Rate Limiting - Setup the egress/ingress rate of packets.
7.Port Lock - Lock ports to prevent the intruder.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Test network integrity and mirroring port.
c.Monitor - Monitor port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.Event Log Table - The complete table of alarm events list.
f.Exit - Exit console menu.
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

8. After entering the Main Menu, use the following keys to move the cursor, and to select options.

Key	Function
Up/Down/Left/Right arrows, or Tab	Move the onscreen cursor
Enter	Display & select options
Space	Toggle options
Esc	Previous Menu

Using the Telnet Console

You may use Telnet to access MOXA EtherDevice Switch's console utility over a network. To be able to access EDS's functions over the network (by Telnet or Web Browser) from a PC host that is connected to the same LAN as EDS, you need to make sure that the PC host and EDS are on the same logical subnetwork. To do this, check your PC host's IP address and netmask. By default, EDS's IP address is 192.168.127.253 and EDS's netmask is 255.255.0.0 (for a Class B network). If you do not change these values, and your PC host's netmask is 255.255.0.0, then its IP address must have the form 192.168.xxx.xxx. On the other hand, if your PC host's netmask is 255.255.255.0, then its IP address must have the form 192.168.127.xxx.

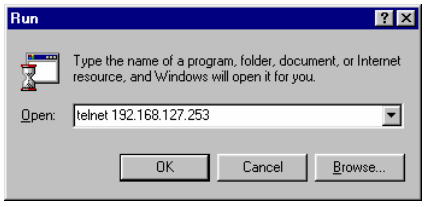
NOTE To use EDS's management and monitoring functions from a PC host connected to the same LAN as EDS, you must make sure that the PC host and EDS are on the same logical subnetwork.

NOTE Before accessing the console utility via Telnet, first connect one of MOXA EtherDevice Switch's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You should be able to establish a connection by using either a straight-through or cross-over Ethernet cable. However, if you experience connection difficulties, refer to the Auto MDI/MDI-X Connection section from of the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

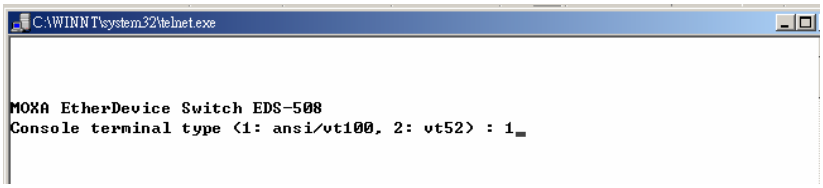
NOTE MOXA EtherDevice Switch's default IP is 192.168.127.253.

Follow the steps below to access the console utility via Telnet.

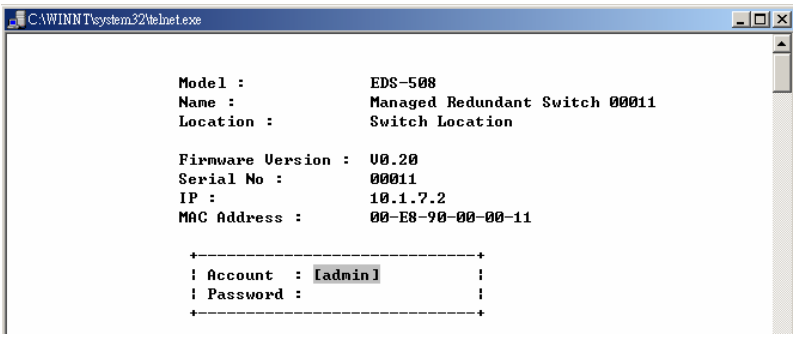
1. Telnet to MOXA EtherDevice Switch's IP address from the Windows **Run** window (or from the MS-DOS prompt).



2. Type **1** to choose **ansi/vt100**, and then press **Enter**.

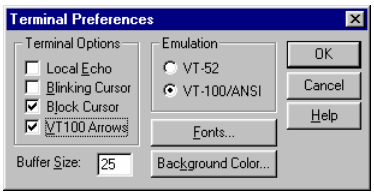


3. If a password has been set for this device, the Console login screen will appear. Enter the **Console Password** (this is the same as the Web Browser password), and then press **Enter**.



4. When MOXA EtherDevice Switch's **Main Menu** opens, select **Preferences…** under the **Terminal** menu.

5. When the **Terminal Preferences** window opens, make sure that the **VT100 Arrows** box is checked.



NOTE The Telnet Console looks and operates in precisely the same manner as the RS-232 Console.

Using Web Configuration

MOXA EtherDevice Switch's web browser interface provides a convenient way to modify the switch's configuration, and to access the built-in monitoring and network administration functions. You may use either Internet Explorer or Netscape to access EDS.

NOTE To use EDS's management and monitoring functions from a PC host connected to the same LAN as EDS, you must make sure that the PC host and EDS are on the same logical subnetwork.

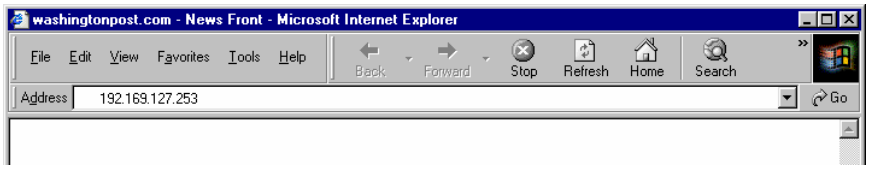
NOTE If EDS is configured for other VLAN settings, you must make sure your PC host is on the management VLAN. Refer to the "Configuring 802.1Q VLAN" in Chapter 3 for the VLAN settings.

NOTE Before accessing MOXA EtherDevice Switch's web browser interface, first connect one of MOXA EtherDevice Switch's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You should be able to establish a connection by using either a straight-through or cross-over Ethernet cable. However, if you experience difficulties, refer to the Auto MDI/MDI-X Connection section of the Hardware Installation Guide for more information.

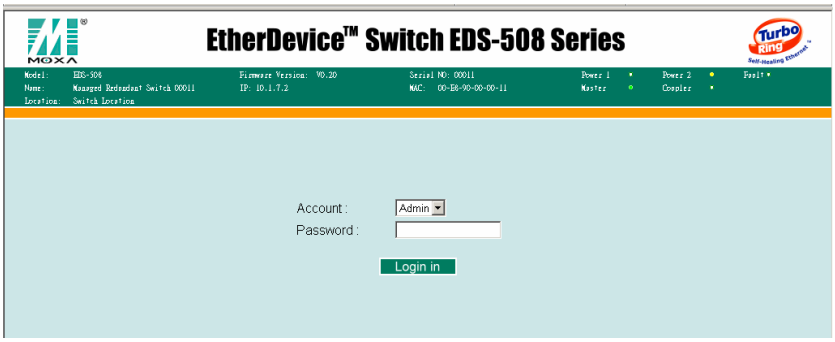
NOTE MOXA EtherDevice Switch's default IP is 192.168.127.253.

Follow the steps below to access MOXA EtherDevice Switch's web browser interface.

1. Start Internet Explorer, and then type the MOXA EtherDevice Switch's IP address in the **Address** field. Press **Enter** to establish the connection.

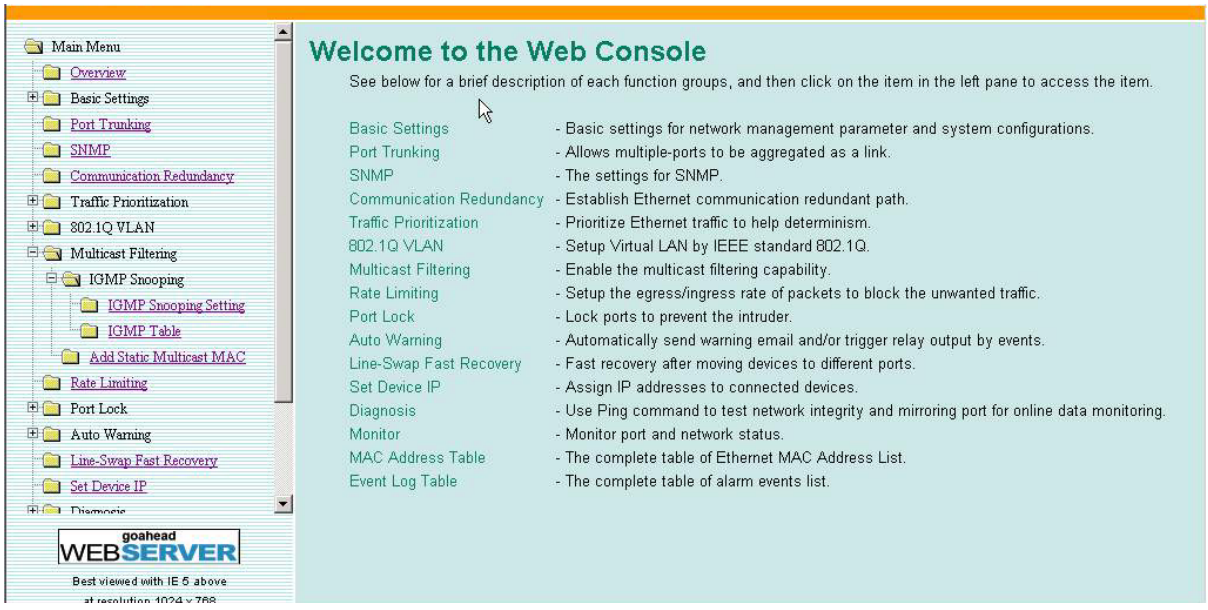

washingtonpost.com - News Front - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search
Address 192.169.127.253
Go

2. The web login page will open. Select the login account (Admin or User) and enter the **Password** (this is the same as the Console password), and then click **Login** to continue.



NOTE MOXA EtherDevice Switch's default Password is not set (i.e., is blank).

You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree in the left side to open the function pages to access each function of MOXA EtheDevice Switch.


Main Menu
Overview
Basic Settings
Port Trunking
SNMP
Communication Redundancy
Traffic Prioritization
802.1Q VLAN
Multicast Filtering
IGMP Snooping
IGMP Snooping Setting
IGMP Table
Add Static Multicast MAC
Rate Limiting
Port Lock
Auto Warning
Line-Swap Fast Recovery
Set Device IP
goahead
WEBSERVER
Best viewed with IE 5 above
Welcome to the Web Console
See below for a brief description of each function groups, and then click on the item in the left pane to access the item.
Basic Settings - Basic settings for network management parameter and system configurations.
Port Trunking - Allows multiple-ports to be aggregated as a link.
SNMP - The settings for SNMP.
Communication Redundancy - Establish Ethernet communication redundant path.
Traffic Prioritization - Prioritize Ethernet traffic to help determinism.
802.1Q VLAN - Setup Virtual LAN by IEEE standard 802.1Q.
Multicast Filtering - Enable the multicast filtering capability.
Rate Limiting - Setup the egress/ingress rate of packets to block the unwanted traffic.
Port Lock - Lock ports to prevent the intruder.
Auto Warning - Automatically send warning email and/or trigger relay output by events.
Line-Swap Fast Recovery - Fast recovery after moving devices to different ports.
Set Device IP - Assign IP addresses to connected devices.
Diagnosis - Use Ping command to test network integrity and mirroring port for online data monitoring.
Monitor - Monitor port and network status.
MAC Address Table - The complete table of Ethernet MAC Address List.
Event Log Table - The complete table of alarm events list.

NOTE If you are connecting MOXA EtherDevice Switch to a public network, but do not intend to use its management functions over the network, then we suggest disabling both **Telnet Console** and **Web Configuration** from the RS-232 Console's **Basic Settings → System Identity** page. See Chapter 3 for details.

3

Featured Functions

This chapter explains how to access MOXA EtherDevice Switch's various configuration, monitoring, and administration functions. There are three ways to access these functions: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect MOXA EtherDevice Switch to a PC's COM port, can be used if you do not know MOXA EtherDevice Switch's IP address. The Telnet console and web browser connection methods can be used to access MOXA EtherDevice Switch over an Ethernet LAN, or over the Internet.

The Web Console is the most user-friendly way to configure MOXA EtherDevice Switch. In this chapter, we use the Web Console interface to introduce the functions. There are only a few differences between the Web Console, Serial Console, and Telnet Console.

The following topics are covered:

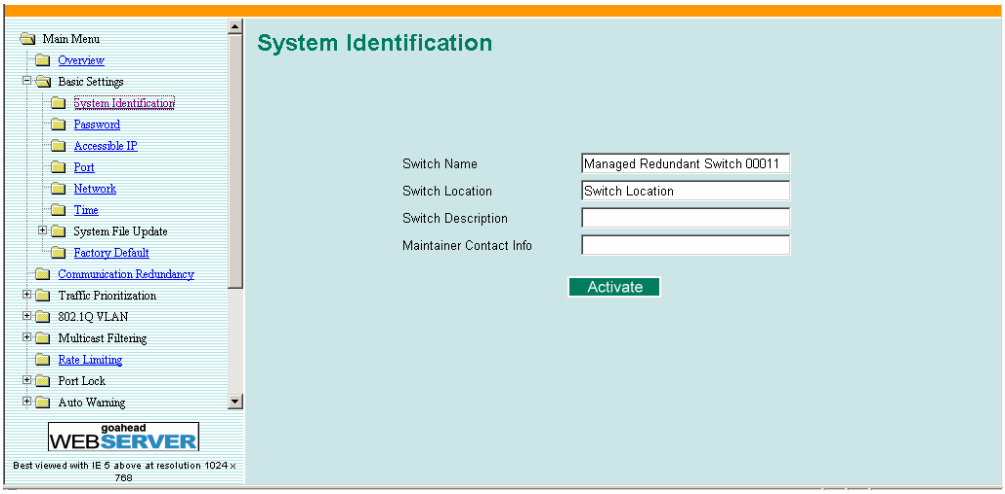
- **Configuring Basic Settings**
- **Using Port Trunking**
- **Configuring Port Trunking**
- **Using SNMP**
- **Using Communication Redundancy**
- **Using Traffic Prioritization**
- **Using Virtual LAN**
- **Using Multicast Filtering**
- **Using Rate Limiting**
- **Using Port Lock**
- **Using Auto Warning**
- **Using Line-Swap-Fast-Recovery**
- **Using Set Device IP**
- **Using Diagnosis**
- **Using Monitor**
- **Using the MAC Address Table**
- **Using Event Log**

Configuring Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control MOXA EtherDevice Switch.

System Identification

The system identification items are displayed at the top of the web page, and will be included in alarm emails. Setting system identification items makes it easier to identify the different switches connected to your network.



Switch Name

Setting	Descriptions	Factory Default
Max. 30 Characters	This option is useful for specifying the role or application of different EDS units. E.g., Factory Switch 1.	"Industrial Redundant Switch [*Serial No. of this switch*]"

Switch Location

Setting	Descriptions	Factory Default
Max. 80 Characters	To specify the location of different EDS units. E.g., production line 1.	"Switch Location"

Switch Description

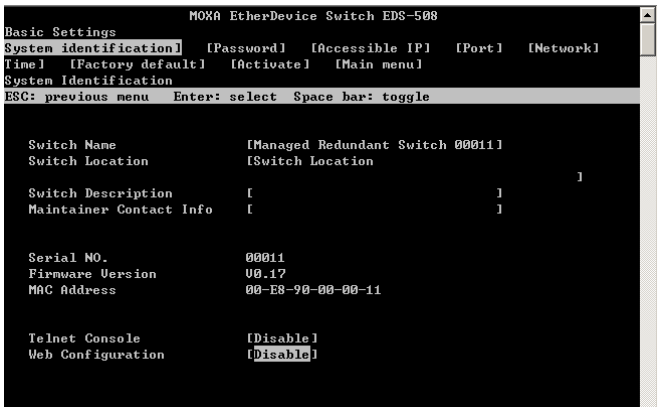
Setting	Descriptions	Factory Default
Max. 30 Characters	For a more detailed description about different EDS units.	None

Maintainer Contact Info

Setting	Descriptions	Factory Default
Max.30 Characters	To provide information about whom to contact in order to resolve problems.	None

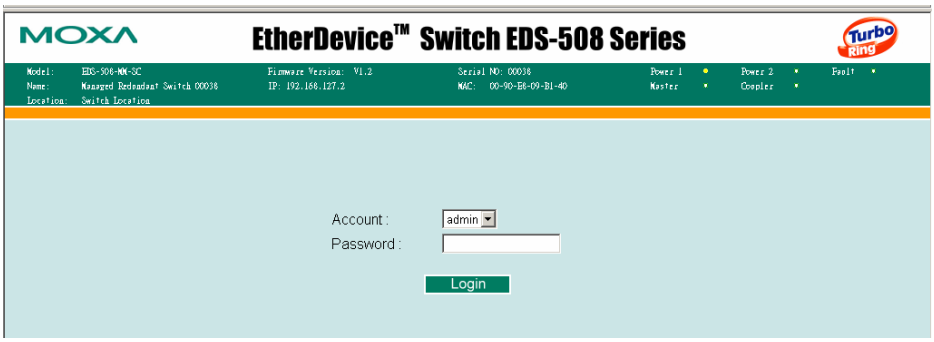
Disable Telnet/Web Console

If you are connecting MOXA EtherDevice Switch to a public network, but do not intend to use its management functions over the network, then we suggest disabling both **Telnet Console** and **Web Configuration** from the RS-232 Console's **Basic Settings → System Identity** page


MOXA EtherDevice Switch EDS-508
Basic Settings
System identification] [Password] [Accessible IP] [Port] [Network]
Time] [Factory default] [Activate] [Main menu]
System Identification
ESC: previous menu Enter: select Space bar: toggle
Switch Name [Managed Redundant Switch 00011]
Switch Location [Switch Location
Switch Description [ ]
Maintainer Contact Info [ ]
Serial NO. 00011
Firmware Version V0.17
MAC Address 00-E8-90-00-00-11
Telnet Console [Disable]
Web Configuration [Disable]

Password

There are two levels of privilege for different users to access EtherDevice Switch. a**Admin** privilege allows access, plus the right to modify ALL EDS configurations. **user** privilege only allows viewing of the configuration, but not the right to make modifications.



ATTENTION

MOXA EtherDevice Switch's default Password is not set (i.e., is blank). If a Password is already set, then you will be required to type the Password when logging into either the RS-232 Console, Telnet Console, or Web Browser interface.

Account Name

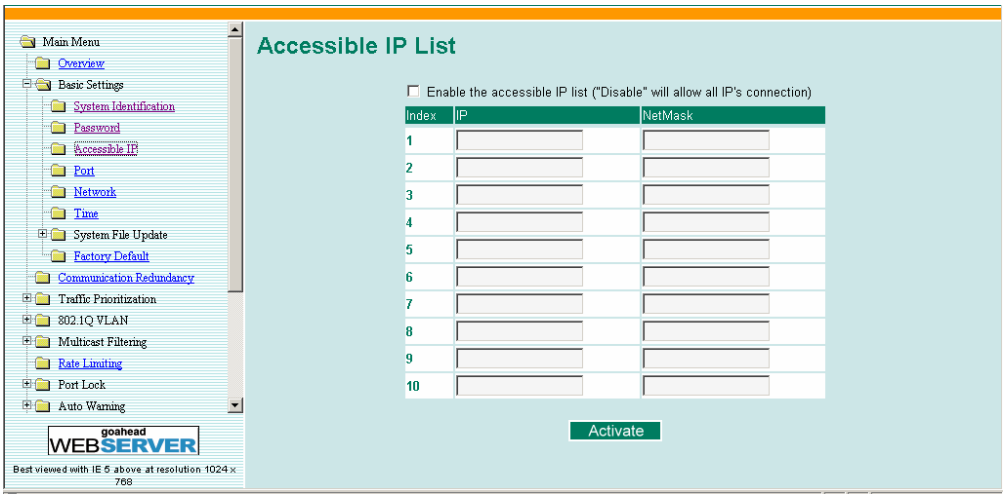
Setting	Descriptions	Factory Default
admin	Admin privilege allows modification of all EDS configurations.	admin
user	User privilege only allows viewing EDS configurations.	

Password Setting

Setting	Descriptions	Factory Default
Old Password (Max. 16 Characters)	Type current password when changing the password	None
New Password (Max. 16 Characters)	Type new password when changing the password	None
Retype Password (Max. 16 Characters)	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Accessible IP

Moxa EtherDevice Switches use an IP address-based filtering method to control access to the EDS.



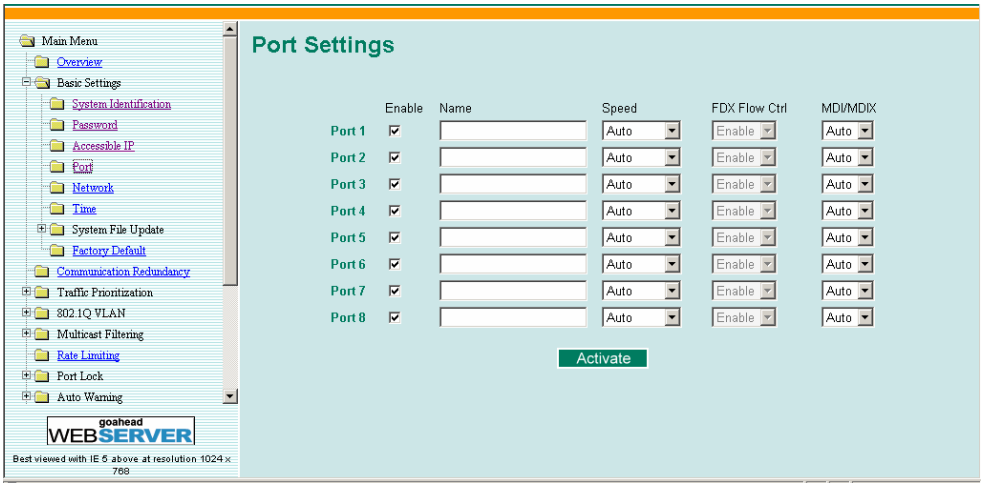
Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to EtherDevice Switch is controlled by IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed access to the EtherDevice Switch. You can allow one of the following cases by setting this parameter

- **Only one host of specific IP address can access the NE-4000T**
  Enter "IP address/255.255.255.255" (e.g., "192.168.1.1/255.255.255.255")
- **Hosts on the specific subnet can access the NE-4000T**
  Enter "IP address/255.255.255.0" (e.g., "192.168.1.0/255.255.255.0")
- **Any host can access the NE-4000T**
  Disable this function. Refer to the following table for more configuration examples.

Allowable Hosts	Input format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Port

The **Port** settings are included to give the user control over Port Access, Port Transmission Speed, Flow Control and Port Type (MDI or MDIX). An explanation of each configuration item is given below.



Enable/Disable Port

Setting	Descriptions	Factory Default
Enable	Choose this option to allow data transmission through the port.	All ports are enabled
Disable	Choose this option to immediately shut off port access.	

ATTENTION

If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option under **Advanced Settings/Port** gives the administrator a quick way to immediately shut off access through this port.

Name

Setting	Descriptions	Factory Default
Max. 63 Characters	To specify the alias of each port and assist the administrator in remembering the important notice related to the port. E.g., PLC 1	None

Port Transmission Speed

Setting	Descriptions	Factory Default
Auto-nego	Allows the port to negotiate with connected devices according to IEEE 802.3u. The port and connected device will determine the best match.	Auto-nego
100M-Full	Choose one of these fixed speed options if the opposing Ethernet device has trouble auto-negotiating for line speed.	
100M-Half		
10M-Full		
10M-Half		

Port Type

Setting	Descriptions	Factory Default
Auto	Allows the port to auto detect the port type of the opposing Ethernet device and change the port type accordingly.	Auto
MDI	Choose the MDI or MDIX option if the opposing Ethernet device has trouble auto-negotiating for port type.	
MDIX		

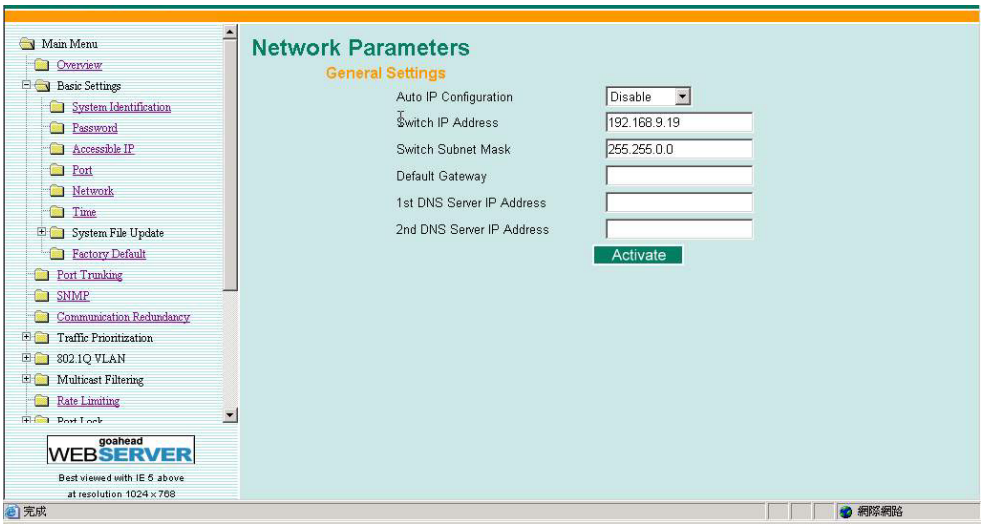
FDX Flow Control

This setting enables or disables the flow control capability of this port when the "port transmission speed" setting is in "auto-nego" mode. The final result will be determined by the auto-nego process between EDS and connected device.

Setting	Descriptions	Factory Default
Enable	Enables the flow control capability of this port when in auto-nego mode.	Enable
Disable	Disables the flow control capability of this port when in auto-nego mode.	

Network

The **Network** configuration allows users to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below.



Auto IP Configuration

Setting	Descriptions	Factory Default
Disable	To set up MOXA EtherDevice Switch's IP address manually.	Disable
By DHCP	To have MOXA EtherDevice Switch's IP address assigned automatically by your network's DHCP server.	
By BootP	To have MOXA EtherDevice Switch's IP address automatically assigned by your network's BootP server.	

Switch IP Address

Setting	Descriptions	Factory Default
IP Address of the EDS	To identify MOXA EtherDevice Switch on a TCP/IP network.	192.168.127.253

Switch Subnet Mask

Setting	Descriptions	Factory Default
Subnet mask of the EDS	To identify the type of network MOXA EtherDevice Switch is connected to. Enter 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network.	255.255.255.0

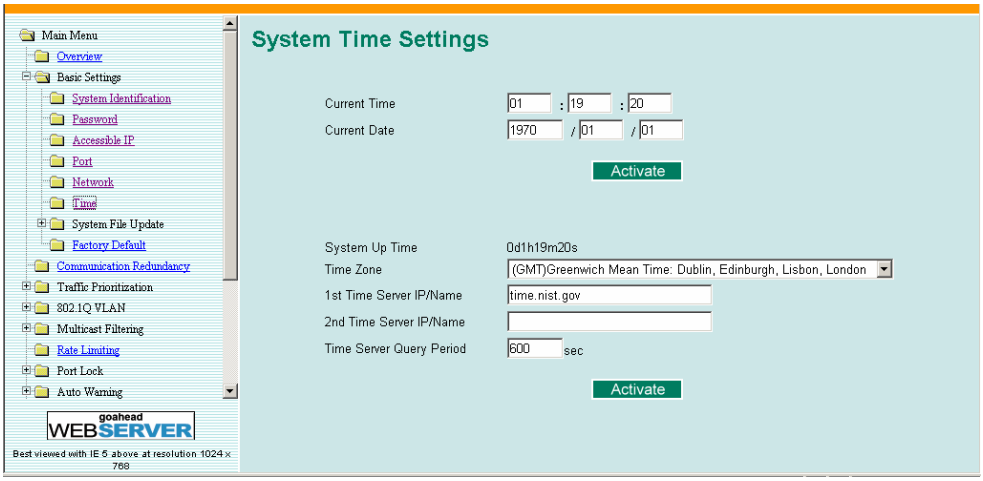
Default Gateway

Setting	Descriptions	Factory Default
Default Gateway of the EDS	Enter your router's IP address if your LAN connects to an outside network.	None

DNS IP Address

Setting	Descriptions	Factory Default
1st DNS Server's IP Address	Enter the IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input MOXA EtherDevice Switch's url (e.g., www.eds.company.com) in your browser's address field, instead of entering the IP address.	None
2nd DNS Server's IP Address	Enter the IP address of the DNS Server used by your network. EtherDevice Switch will try to locate the 2nd DNS Server if the 1st DNS Server fails to connect.	None

Time



EtherDevice Switch has a time calibration function based on information from an NTP server or user specified Time and Date information. Functions such as Auto warning "Email" can add real-time information to the message.

NOTE EDS does not have a real time clock. The user must update the **Current Time** and **Current Date** to set the initial time for EDS after each reboot, especially when the network doesn't have an Internet connection for NTP server or there is no NTP server on the LAN.

Current Time

Setting	Description	Factory Default
User adjustable time.	The time parameter allows configuration of the local time in local 24-hour format.	00h:00m:00s

Current Date

Setting	Description	Factory Default
User adjustable date.	The date parameter allows configuration of the local date in yyyy-mm-dd format.	1970/01/01

System Up Time

Indicates EtherDevice Switch's up time from last cold start. The unit is seconds.

Time Zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

NOTE Changing the time zone will automatically correct the current time. It is recommended that **the time zone be configured before the time is set**.

Time Server IP/Name

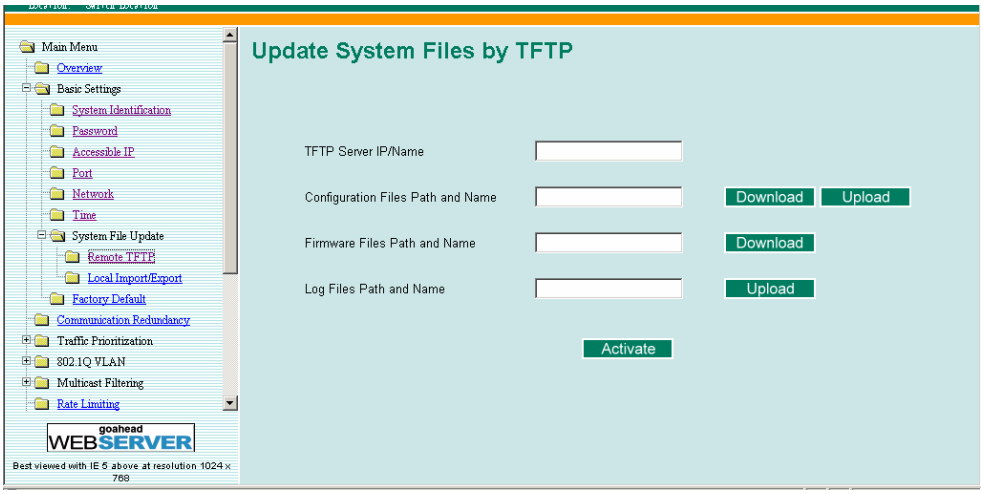
Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (E.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov)	None
2nd Time Server IP/Name	EtherDevice Switch will try to locate 2nd NTP Server if the 1st NTP Server fails to connect.	

Time Server Query Period

Setting	Description	Factory Default
Query Period	This parameter determines how frequently the time is updated from the NTP server.	600 seconds

System File Update—By Remote TFTP

MOXA EtherDevice Switch supports saving your configuration file to a remote TFTP server or local host to allow other EtherDevice Switches to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported for easy upgrading or configuration of the EtherDevice Switch.



TFTP Server IP/Name

Setting	Description	Factory Default
IP Address of TFTP Server	The IP or name of the remote TFTP server. Must be set up before downloading or uploading files.	None

Configuration file path and name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of EtherDevice Switch's configuration file in the TFTP server.	None

Firmware file path and name

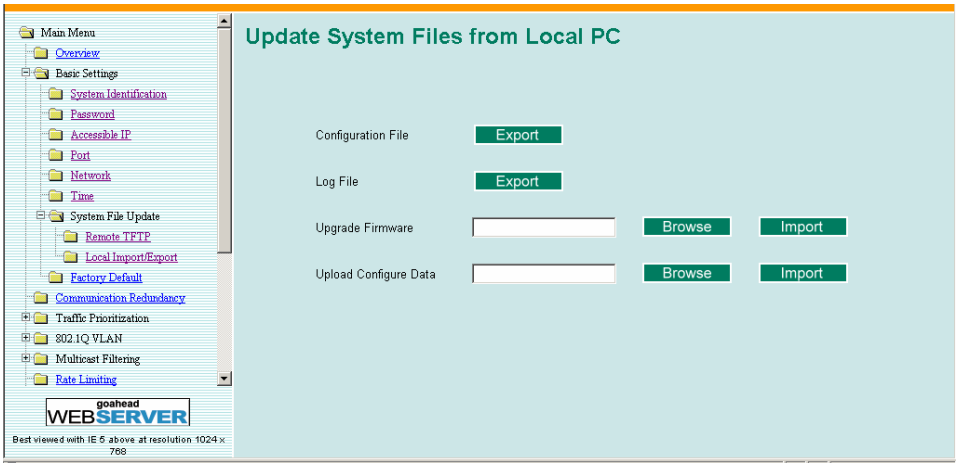
Setting	Description	Factory Default
Max. 40 Characters	The path and file name of EtherDevice Switch's firmware file.	None

Log file path and name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of EtherDevice Switch's log file	None

After setting up the desired path and file name, click on **Activate** to save the setting, and then click on **Download** to download the prepared file from the remote TFTP server, or click on **Upload** to upload the desired file from the remote TFTP server.

System File Update—By Local Import/Export



Configuration File Export

To export the configuration file of this EDS, click on **Export** to save it to the local host.

Log File Export

To export the Log file of this EDS, click on **Export** and save it to the local host.

NOTE Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click on the "Export" button to save a file.

Firmware Import

To import the firmware file of this EDS, click on **Browse** to open the file browse window to select the firmware already saved on this computer. The upgrade procedure will proceed automatically after clicking on **Import**.

Configuration File Import

To import the configuration file of this EDS, click on **Browse** to open the file browse window to select the configuration file already saved on this computer. The upgrade procedure will proceed automatically after clicking on **Import**.

Factory Default

The Factory Default function is included to give users a quick way of restoring MOXA EtherDevice Switch's configuration settings to their factory default values. This function can be accessed from either the Console utility or Web Browser interface.

NOTE After activating the Factory Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your MOXA EtherDevice Switch.

Using Port Trunking

Port Trunking allows devices to communicate by aggregating up to four links in parallel and a maximum of 4 ports for each link. This means that users could connect one EDS to another EDS by port trunking to double, triple or quadruple the bandwidth of the connection.

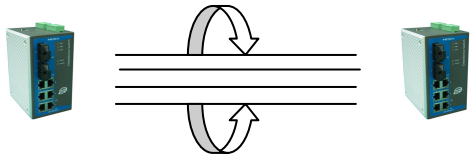
The Concept of Port Trunking

Moxa developed the proprietary port trunking protocol to provide the following benefits:

- Provide a flexible network connection by doubling, tripling, or quadrupling the bandwidth of a link.
- Providing redundancy—if one link is broken, the other ports share the traffic within this link.

Port trunking can aggregate up to four ports between two EDSs. If all ports on both Switch units are configured as 100BASE-TX and they are operating in full duplex, the potential bandwidth of the connection will be 800 Mbps.

Aggregate up to four ports into a port trunking configuration



Port Trunking
800 Mbps

When configuring port trunking, note that:

- Each EDS can use a maximum of 4 Port trunking groups (designated Trk1, Trk2, Trk3, Trk4)
- Each port trunking group uses between 1 and 4 ports
- All ports belonging to one port trunking group must be set to the same speed. E.g., 100 M Full, 100M Half, 10M Full, or 10M Half. The auto-negotiation function should be disabled.

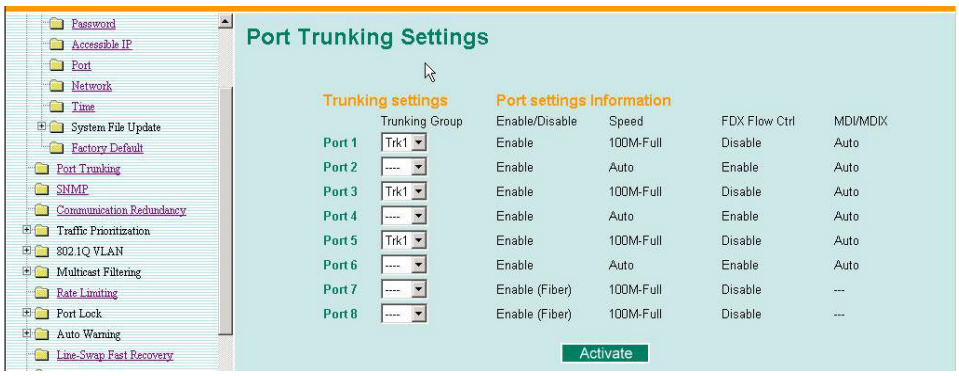
When you activate port trunking settings, some advanced functions will either be set to factory default values, or disabled:

- **Communication Redundancy** will be set to the factory default
- **802.1Q VLAN** will be set to the factory default and will be disabled
- **Multicast Filtering** will be set to the factory default
- **Port Lock** will be set to the factory default and will be disabled
- **Set Device IP** will be set to the factory default
- **Mirror** will be set to the factory default and will be disabled

Configuring Port Trunking

Port Trunking Settings

The following figures indicate which Port Trunking Setting parameters can be configured. A more detailed explanation of each parameter is given below the figure.



Trunking settings

Setting	Descriptions	Factory Default
----	Do not select this port to join port trunking groups	None
Trk1	Select this port to join port trunking group 1	None
Trk2	Select this port to join port trunking group 2	None
Trk3	Select this port to join port trunking group 3	None
Trk4	Select this port to join port trunking group 4	None

Port setting information

Enable/Disable

Indicates if this port is "Enabled" or "Disabled."

Port Transmission Speed

Indicates the transmission speed status as 100M-Full, 100M-Half, 10M-Full, or 10M-Half.

FDX Flow Control

Indicates if the FDX flow control of this port is "Enabled" or "Disabled."

Port Type

Indicates that the port type for this port is Auto, MDI, or MDIX.

Using SNMP

EDS supports three SNMP protocols. The available protocols are SNMP V1, SNMP V2c, and SNMP V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means SNMP servers access all objects with read-only or read/write permissions using the community string *public/private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol.. You can also enable data encryption to enhance data security.

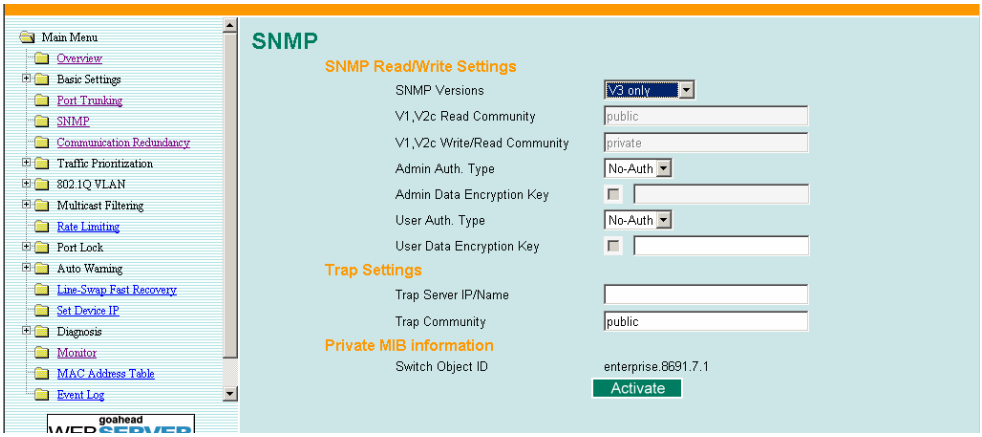
SNMP security modes and security levels supported by EDS are shown in the following table. Select one to communicate between the SNMP agent and manager

Protocol Version	Security Mode	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

Configuring SNMP

SNMP Read/Write Settings

The following figures indicate which SNMP parameters can be configured. A more detailed explanation of each parameter is given below the figure



SNMP Versions

Setting	Descriptions	Factory Default
V1, V2c, V3	Select SNMP Versions V1, V2c, V3 protocol to manage the switch	V1, V2c
V1, V2c	Select SNMP Versions V1, V2c protocol to manage the switch	
V3 only	Select SNMP Versions V3 protocol only to manage the switch	

V1, V2c Read Community

Setting	Descriptions	Factory Default
V1, V2c Read Community	Use a community string match for authentication, which means that the SNMP agent accesses all objects with read-only permissions using the community string *public*.	public Maximum 30 characters

V1, V2c Read/Write Community

Setting	Descriptions	Factory Default
V1, V2c Read/Write Community	Uses a community string match for authentication, which means that SNMP servers access all objects with read/write permissions using the community string *private.*	private Maximum 30 characters

For SNMP V3, there are two levels of privilege for different accounts to access the EDS. **Admin** privilege allows access and authorized to read and write MIB file. **User** privilege only allows reading MIB file, but not authorized to write

Admin Auth. Type (For SNMP V1, V2c, V3 and V3 only)

Setting	Descriptions	Factory Default
No-Auth	Use admin. account to access objects. No authentication	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

Admin Data Encryption Key (For SNMP V1, V2c, V3 and V3 only)

Setting	Descriptions	Factory Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key	No
Disable	No data encryption	No

User Auth. Type (For SNMP V1, V2c, V3 and V3 only)

Setting	Descriptions	Factory Default
No-Auth	Use account of admin or user to access objects. No authentication	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

User Data Encryption Key (For SNMP V1, V2c, V3 and V3 only)

Setting	Descriptions	Factory Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key.	No
Disable	No data encryption	No

Trap Settings

Setting	Descriptions	Factory Default
Trap Server IP/Name	Enter the IP address or name of the Trap Server used by your network.	None
Trap Community	Use a community string match for authentication; Maximum of 30 characters.	public

Private MIB information

The private SNMP Object ID of the EDS is the enterprise value: 8691.7.1. This number is cannot be changed.

Using Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and reduces network downtime to a minimum.

The Communication Redundancy function allows the user to set up *redundant loops* in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if MOXA EtherDevice Switch is used as a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. MOXA Ethernet Device Switch supports two different protocols to support this communication redundancy function—**Rapid Spanning Tree Protocol (IEEE-802.1W)** and **Turbo Ring**.

Turbo Ring and STP/RSTP cannot both be used on the network at the same time. The table below lists the key differences between each feature, so you can evaluate the benefits of each to determine which feature is most suitable for your network.

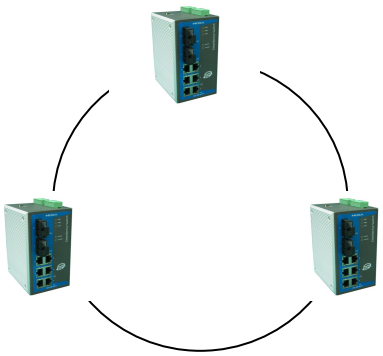
	Turbo Ring	STP	RSTP
Topology	Ring	Ring, Mesh	Ring, Mesh
Recovery Time	< 300 ms	Up to 30 sec.	Up to 5 sec

The Concept of Turbo Ring

Moxa developed the proprietary Turbo Ring protocol to optimize communication redundancy and achieve a faster recovery time on the network.

Turbo Ring protocol identifies one switch as the "master" of the network, and then automatically blocks packets from traveling through any of the network's redundant loops. In the event that one branch of this ring becomes disconnected from the rest of the network, the Turbo Ring protocol automatically readjusts the ring (if possible) so that the part of the network that was disconnected can reestablish contact with the rest of the network.

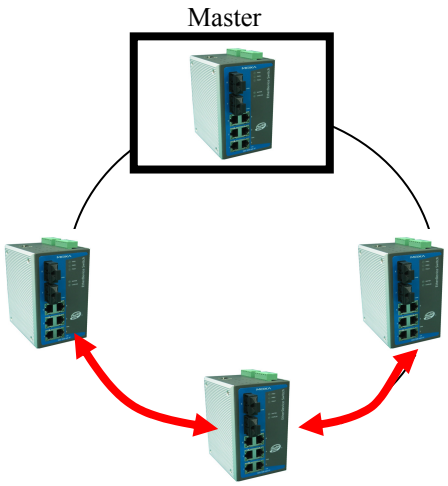
Initial Setup



1. Select any two ports as redundant ports.
2. Connect the redundant ports to form the Turbo Ring

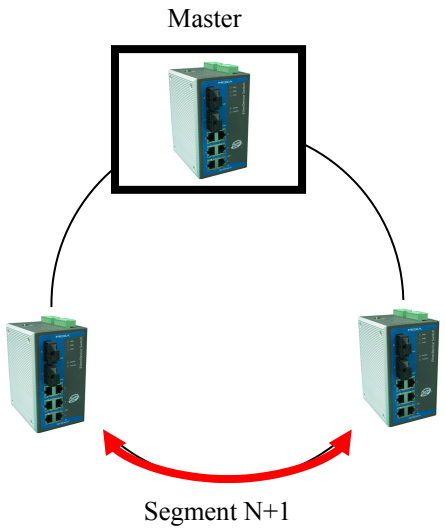
The user does not need to set the master to use Turbo Ring. Master is only needed to identify which segment acts as the backup path. The actual topology of the redundant ring, i.e., which segment will be blocked, is determined by the number of EDSs that make up the ring and where the "Ring Master" is located.

When the number of EDS units in the Turbo Ring is even.



If there are 2N EDS units (an even number) in the Turbo Ring, then the backup segment is one of the two segments connected to the (N+1)st EDS (i.e., the EDS unit directly opposite the Master).

When the number of EDS units in the Turbo Ring is odd.



If there are 2N+1 EDS units (an odd number) in the Turbo Ring, with EDS units and segments labeled counterclockwise, then segment N+1 will serve as the backup path.

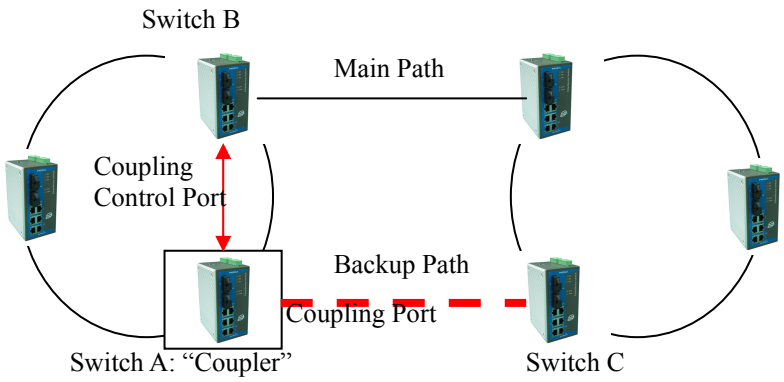
For the example shown here, N=1, so that N+1=2.

For some systems, it may not be convenient to connect all devices in the system to make one BIG redundant ring, since some devices could be located in a remote area. The "Ring Coupling" function of Turbo Ring can help you separate those distributed devices into different smaller redundant rings, but in such a way that they can still communicate with each other. The figure below illustrates how to couple two Turbo Rings.

ATTENTION

In the VLAN environment, the user has to set "Redundant Port," "Coupling Port," and "Coupling Control Port" as "Trunk Port." Since these ports act as the "backbone" to transmit all packets of different VLANs to different EDS units.

Ring Coupling



To support the Ring Coupling function, select one EDS (e.g., Switch A in the above figure) in the Turbo Ring and enter the Communication Redundancy page to enable "Ring Coupling." Select one port as "coupling port" and then connect any port of the opposing EDS (e.g., Switch C) in the adjacent Turbo Ring. Select another port as "coupling control port," and connect this port to any port of the adjacent EDS (e.g., Switch B) in the same Turbo Ring.
The "Coupler" switch (Switch A above) will monitor switch B's order from the "coupling control port" to decide if the coupling port's backup path should be recovered.

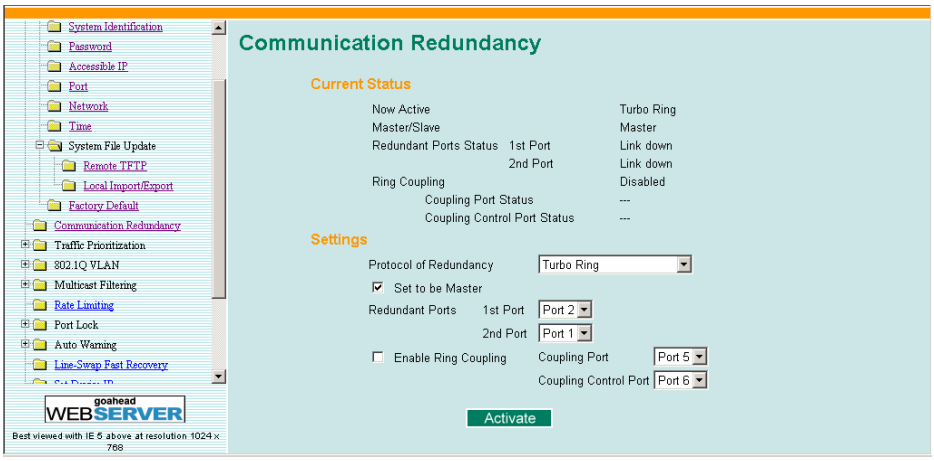
ATTENTION

The user only needs to enable the "Ring Coupling" function in one EDS (not on the opposing EDS or adjacent EDS).
Redundant Ports, Coupling Port and Coupling Control Port should be configured as among four individual port.

NOTE Ring Coupling and Ring Master do not need to be set up on the same EDS.

Configuring Turbo Ring

The following figures indicate which Turbo Ring Protocol parameters can be configured. A more detailed explanation of each parameter is given below the figure.



Now Active:

This field shows which communication protocol is on used: Turbo Ring, RSTP, or neither.

Master/Slave:

This field appears only when selected to operate in Turbo Ring mode. It indicates if this EDS is or is not the Master of the Turbo Ring.

NOTE The user does not need to set the master to use Turbo Ring, only to assign which segment serves as the backup path.
The master will be determined automatically if the user does not set a dedicated master for the Turbo Ring.

Redundant Port Status

This field indicates the current status of redundant ports. The state is "Forwarding" for normal transmission, "Blocked" to stop transmission if this port is the backup path, and "Link down" for non-connection.

Ring Coupling

Indicates if the Ring Coupling function is "Enabled" or "Disabled."

Coupling Port Status

This field indicates the current status of coupling ports. The state is "Forwarding" for normal transmission, "Blocked" to stop transmission if this port is the backup path, and "Link down" for non-connection.

At the bottom of the page, the user can configure this function's "Settings." For Turbo Ring, the user can configure:

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	None

Set as Master

Setting	Description	Factory Default
Enable/Disable	Select this EDS as Master	None

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of EDS to be one of the redundant ports.	Port 7 if enable Turbo Ring
2nd Port	Select any port of EDS to be one of the redundant ports.	Port 8 if enable Turbo Ring

Enable Ring Coupling

Setting	Description	Factory Default
Enable/Disable	Select this EDS as Coupler	None

Coupling Ports

Setting	Description	Factory Default
Coupling Port	Select any port of EDS to be the coupling port	Port 5 if enable Ring Coupling
Coupling Control Port	Select any port of EDS to be the coupling control port	Port 6 if enable Ring Coupling

The Concept of STP/RSTP

The Spanning Tree Protocol (STP) makes your network more resilient to link failure and also provides a protection from loops—one of the major causes of broadcast storms. STP is disabled by default on EDS. To be fully effective, RSTP/STP must be enabled on all EDSs connected to your network.

The Rapid Spanning Tree Protocol (RSTP) is an enhanced Spanning Tree feature. RSTP implements the Spanning Tree Algorithm and Protocol, as defined in the IEEE Std 802.1w-2001. Some of the benefits of RSTP are:

- Faster determination of the topology throughout a bridged network.
- Easy deployment throughout a legacy network, through backward compatibility:
  - Will default to sending 802.1D style BPDU's on a port if it receives packets of this format.
  - It is possible for some ports on an EDS to operate in RSTP (802.1w) mode, and other ports, for example those connected to a legacy switch, to operate in STP (802.1D) mode.

RSTP provides the same functionality as STP. For details on how the two systems differ, see the *How RSTP Differs from STP* section in this chapter. The following sections explain more about

STP and the protocol features supported by your EDS.

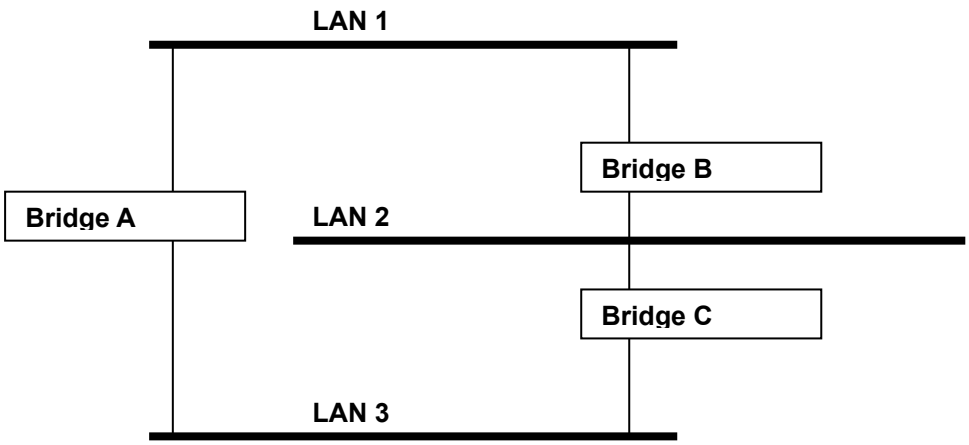
NOTE The protocol is part of the IEEE Std 802.1D, 1998 Edition bridge specification. The following explanation of STP uses bridge instead of switch.

What is STP?

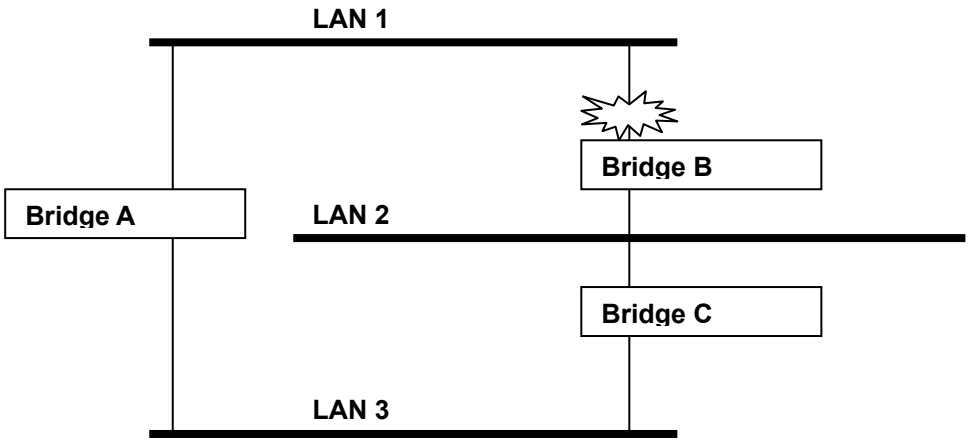
STP (802.1D) is a bridge-based system that allows you to implement parallel paths for network traffic and uses a loop-detection process to:

- Find and disable the less efficient paths (that is, the paths that have a lower bandwidth).
- Enable one of the less efficient paths if the most efficient path fails.

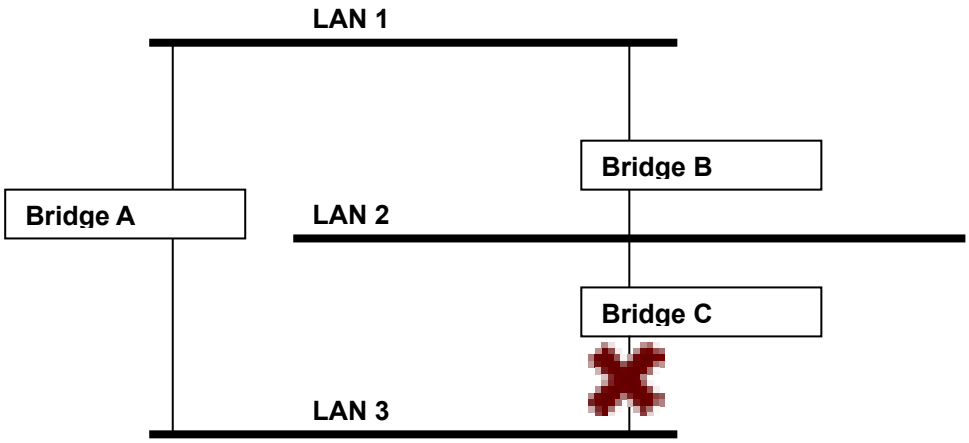
As an example, the figure below shows a network containing three LAN segments separated by three bridges. With this configuration, each segment uses at most two paths to communicate with the other segments. If STP is NOT enabled, this configuration creates loops that cause the network to overload.



The next figure shows the result of enabling STP on the bridges in the configuration. STP detects duplicate paths and prevents, or *block*s, one of them from forwarding traffic, so that the configuration will work satisfactorily. STP could have determined, for example, that traffic from LAN segment 2 to LAN segment 1 should flow through Bridges C and A because this path has a greater bandwidth and is therefore more efficient.



If a link failure is detected, as shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through Bridge B.



STP determines which path between each bridged segment is the most efficient, and assigns a specific reference point on the network. Once the most efficient path has been determined, all other paths are blocked. Therefore, in the above 3 figures, STP initially determined that the path through Bridge C was the most efficient, and consequently blocked the path through Bridge B. After the failure of Bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

STP Requirements

Before it can configure the network, the STP system requires:

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier

are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. The default priority of EDS is 32768.

- Each port has a cost that specifies the efficiency of each link, usually determined by the bandwidth of the link—the higher the cost, the less efficient the link. The following table shows the default port costs for a Switch:

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP Calculation
The first stage in the STP process is the calculation stage. During this stage, each bridge on the network transmits BPDUs that allow the system to calculate:

- Which bridge should be the Root Bridge. The Root Bridge is the central reference point from which the network is configured.
- The Root Path Costs for each bridge—that is, the cost of the paths from each bridge to the Root Bridge.
- The identity of the port on each bridge that is to be the Root Port. The Root Port is the port connected to the Root Bridge using the most efficient path. That is, the one that has the lowest Root Path Cost. Note that the Root Bridge does not have a Root Port.
- The identity of the bridge that is to be the Designated Bridge of each LAN segment. The Designated Bridge is the one that has the lowest Root Path Cost from that segment. Note that if several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. All traffic destined to pass in the direction of the Root Bridge flows through the Designated Bridge. The port on this bridge that connects to the segment is called the Designated Bridge Port.

STP Configuration
After all the bridges on the network have agreed on the identity of the Root Bridge, and have established the other relevant parameters, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they are prevented from receiving or forwarding traffic.

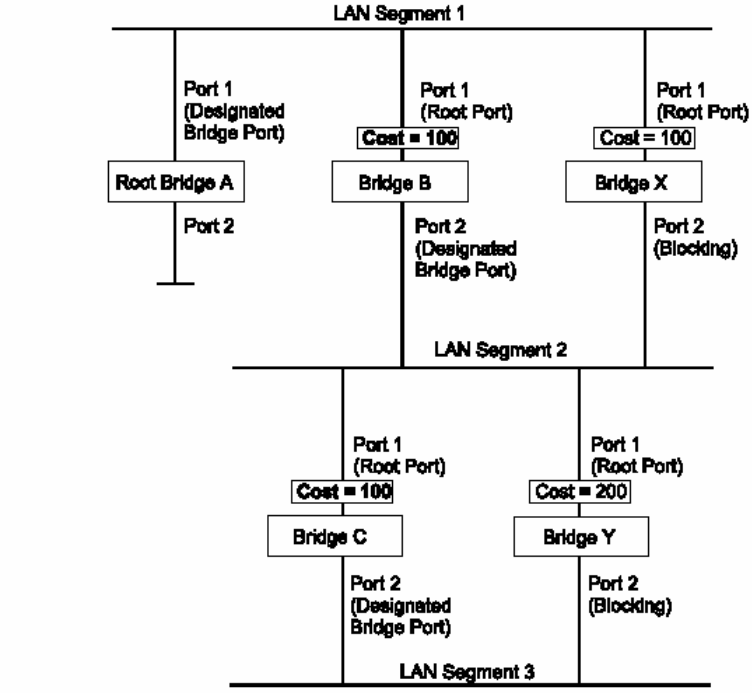
STP Reconfiguration
Once the network topology is stable, all the bridges listen for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. The bridge then reconfigures the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

How RSTP Differs from STP

RSTP works in a similar way to STP, but it includes additional information in the BPDUs. This information allows each bridge to confirm that it has taken action to prevent loops from forming when it wants to enable a link to a neighboring bridge. This allows adjacent bridges connected via point-to-point links to enable a link without needing to wait to ensure that all other bridges in the network have had time to react to the change. So the main benefit of RSTP is that the configuration decision is made locally rather than network-wide, which is why RSTP can carry out automatic configuration and restore a link faster than STP.

STP Example

The figure below shows a LAN that has STP enabled. The LAN has three segments, and each segment is connected using two possible links.



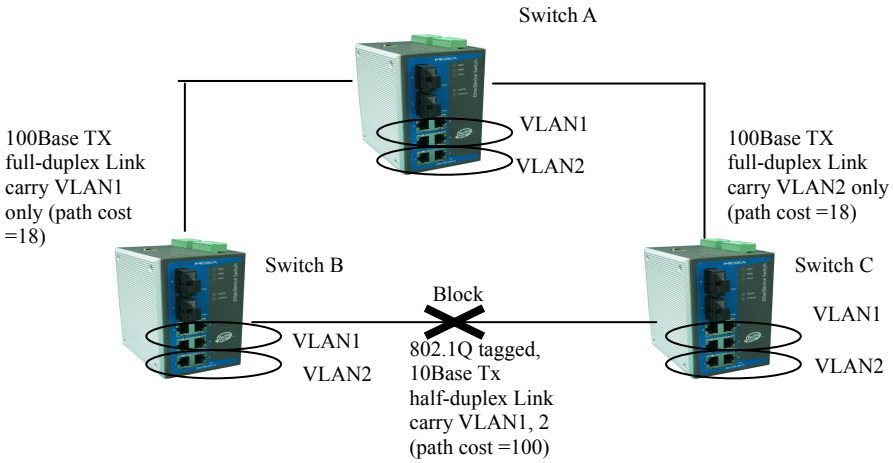
- Bridge A has the lowest Bridge Identifier in the network, and has therefore been selected as the Root Bridge.
- Because Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is therefore selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y have been defined as Root Ports because they are the nearest to the Root Bridge and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B has been selected as the Designated Bridge for the segment because it has a lower Bridge Identifier. Port 2 on Bridge B is therefore selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C has been selected as the Designated Bridge for LAN segment 3, because it offers the lowest Root Path Cost for LAN Segment 3:
  - the route through Bridges C and B costs 200 (C to B=100, B to A=100)
  - the route through Bridges Y and B costs 300 (Y to B=200, B to A=100)

Port 2 on Bridge C is therefore selected as the Designated Bridge Port for LAN Segment 3.

Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when it calculates STP information—the calculations are only performed on the basis of physical connections. For this reason, some network configurations can result in VLANs being subdivided into a number of isolated sections by the STP system. Therefore, you must ensure that any VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may

result from link failures. For example, the following figure shows a network containing VLANs 1 and 2. They are connected using the 802.1Q-tagged link between Switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other Switch-to-Switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on Switch units A and B cannot communicate with VLAN 1 on Switch C, and VLAN 2 on Switch units A and C cannot communicate with VLAN 2 on Switch B.

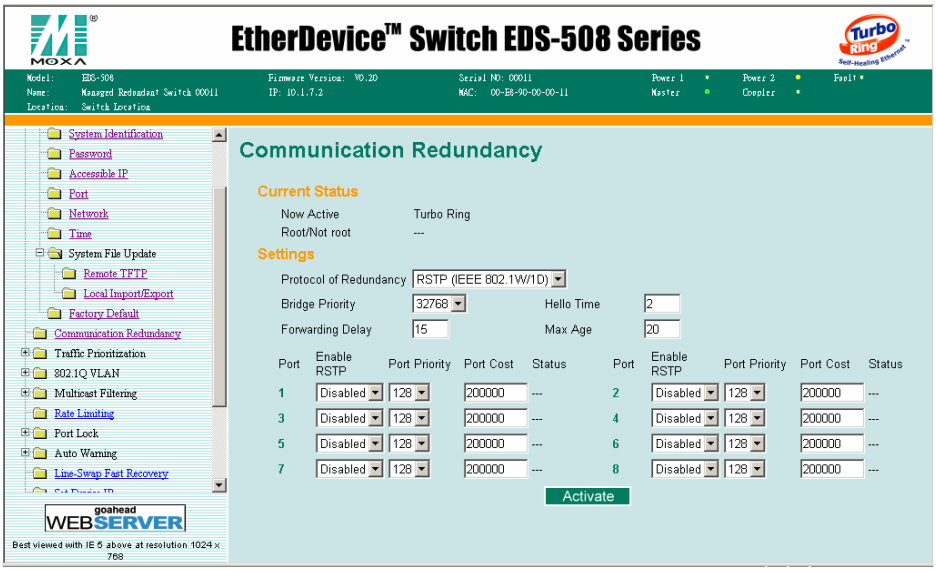


To avoid any VLAN subdivision, it is recommended that all inter-Switch connections are made members of all available 802.1Q VLANs to ensure connectivity at all times. For example, the connections between Switches A and B, and between Switches A and C should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

For more information about VLAN Tagging, see the section Configuring Virtual LANs.

Configuring STP/RSTP

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter is given below.



At the top of this page, the user can check the "Current Status" of this function. For RSTP, you will see:

Now Active:

This field will show which communication protocol is being used—Turbo Ring, RSTP, or neither.

Root/Not Root

This field will appear only when selected to operate in RSTP mode. It indicates if this EDS is or is not the Root of the Spanning Tree (the root is determined automatically).

At the bottom of this page, the user can configure the "Settings" of this function. For RSTP, you can configure:

Protocol of Redundancy

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	None

Bridge priority

Setting	Description	Factory Default
User selectable numbers	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time (sec.)

Setting	Description	Factory Default
User adjustable numbers	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max. Age (sec.)

Setting	Description	Factory Default
User adjustable numbers	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

Enable STP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disable

NOTE We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Port Priority

Setting	Description	Factory Default
User selectable number	Increase this port's priority as a node on the Spanning Tree topology by inputting a lower number.	128

Port Cost

Setting	Description	Factory Default
User adjustable number	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	200000

Port Status

Indicates the current Spanning Tree status of this port. "Forwarding" for normal transmission, "Blocking" to block transmission.

Configuration Limits of RSTP/STP

We should point out that the Spanning Tree Algorithm places certain limits on three of the configuration items described above:

[Eq. 1]: 1 sec $\leqq$ Hello Time $\leqq$ 10 sec

[Eq. 2]: 6 sec $\leqq$ Max. Age $\leqq$ 40 sec

[Eq. 3]: 4 sec $\leqq$ Forwarding Delay $\leqq$ 30 sec

These three variables are further restricted by the following two inequalities:

[Eq. 4]: 2 * (Hello Time + 1 sec) $\leqq$ Max. Age $\leqq$ 2 * (Forwarding Delay – 1 sec)

MOXA EtherDevice Switch's firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

2 * (Hello Time + 1 sec) = 12 sec, and 2 * (Forwarding Delay – 1 sec) = 6 sec.

You can remedy the situation in any number of ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

Using Traffic Prioritization

Using the traffic prioritization capabilities of your EDS provides Quality of Service (QoS) to your network through increased reliability of data delivery. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the Switch. MOXA EtherDevice Switch can inspect both IEEE 802.1p/1Q layer 2 CoS tag, and even layer 3 TOS information to provide consistent classification of the entire network. MOXA EtherDevice Switch Series' QoS capability improves the performance and determinism of industrial networks for mission critical applications.

The Concept of Traffic Prioritization

What is Traffic Prioritization?

Today's application traffic consists of different types of data. When these different types of data compete for the same bandwidth, a network can quickly become overloaded, resulting in slow response times (long latency), and application time-outs. Traffic prioritization is a mechanism that allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- You can control a wide variety of traffic and manage congestion on your network, therefore improving performance.
- You can assign priorities to traffic. For example, set higher priorities for time-critical or business-critical applications.
- You can provide predictable throughput for multimedia applications such as video conferencing or voice over IP, as well as minimize traffic delay and jitter.
- You can improve network performance as the amount of traffic grows, which also reduces the need to constantly add bandwidth to the network, therefore saving cost.

How Traffic Prioritization Works

Traffic prioritization uses the four traffic queues that are present in your EDS to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. This is what provides Quality of Service (QoS) to your network.

EDS traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D**—a layer 2 marking scheme.

- **Differentiated Services (DiffServ)**—a layer 3 marking scheme.

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4 byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns each frame with an IEEE 802.1p priority level between 0 and 7, which determines the level of service that that type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional in Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network has to implement IEEE 802.1Q VLAN tagging.

It is only supported on a LAN and not across routed WAN links, because the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking because you can choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

Advantages of DiffServ over IEEE 802.1D are:

- You can configure how you want your switch to treat selected applications and types of traffic, by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet and therefore priority is preserved across the Internet.
- DSCP is backward compatible with IPV4 TOS, which allows operation with existing devices that are using the layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

EDS classifies traffic based on layer 2 of the OSI 7 layer model, and the Switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority

queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and therefore traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

1. A packet received by the EDS may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be remarked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
2. Because the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.

The EDS will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines which traffic queue the packet is mapped to.

Traffic Queues

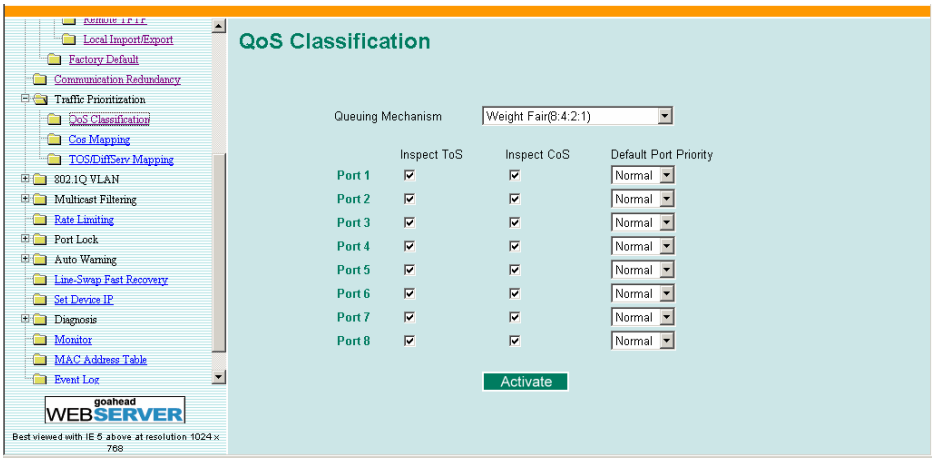
The EDS hardware has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the EDS without being delayed by lower priority traffic. As each packet arrives in the EDS, it passes through any ingress processing (which includes classification, marking/remarking), and is then sorted into the appropriate queue. The Switch then forwards packets from each queue.

EDS supports two different queuing mechanisms:

- Weighted Fair: This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, this method gives high priority precedence over low-priority, but in the event that high-priority traffic exceeds the link capacity, lower priority traffic is not blocked.
- Strict: This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. This method always gives precedence to high priority over low-priority.

Configuring Traffic Prioritization

QoS Classification



MOXA EtherDevice Switch supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	EDS-508 has 4 priority queues. In the weighted fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames to egress the switch as soon as possible.	

Inspect TOS

Setting	Description	Factory Default
Enable/Disable	Check the checkbox to enable EDS-508 to inspect the Type of Service (TOS) bits in IPV4 frame to determine the priority of each frames.	Enable

Inspect COS

Setting	Description	Factory Default
Enable/Disable	Check the check box to enable EDS-508 to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame.	Enable

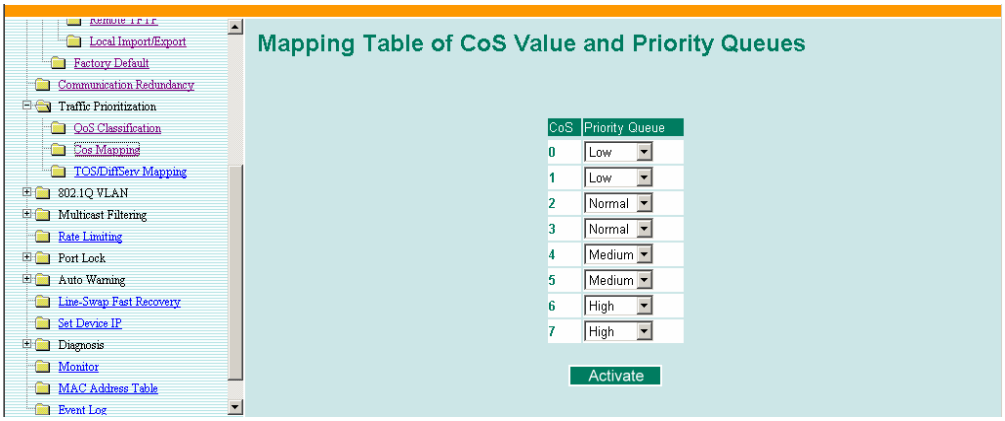
Default Port Priority

Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the Port Default Priority of the ingress frames to different priority queues. If the received packets are not equipped with any tag information (CoS, TOS) the default port priority will take effect.	Normal

NOTE The priority of an ingress frame is determined in order by:
1. Inspect TOS
2. Inspect CoS
3. Default Port Priority

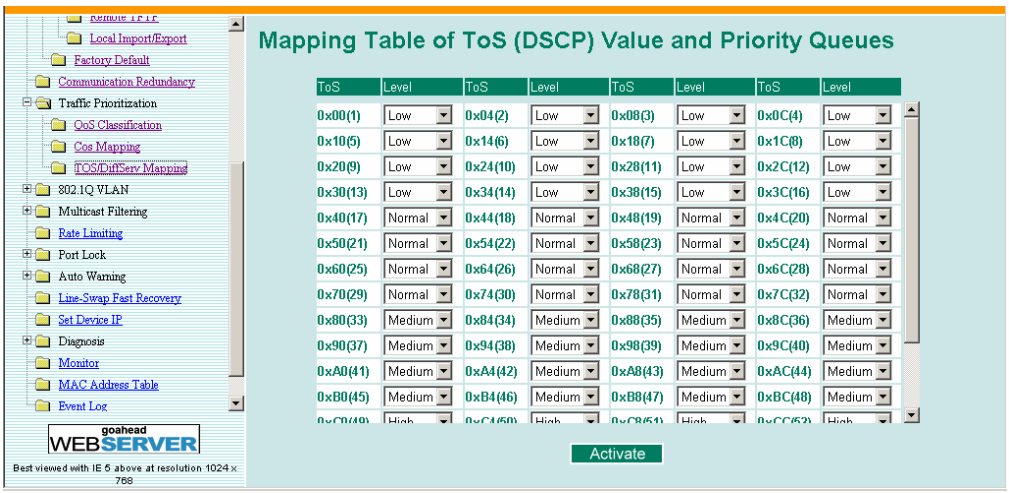
NOTE The designer can enable these classifications individually or in combination. For instance, if a 'hot,' higher priority port, is required for a network design, "Inspect TOS" and "Inspect CoS" can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

CoS Mapping



Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the mapping table of different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

TOS/DiffServ Mapping



Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the mapping table of different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

Using Virtual LAN

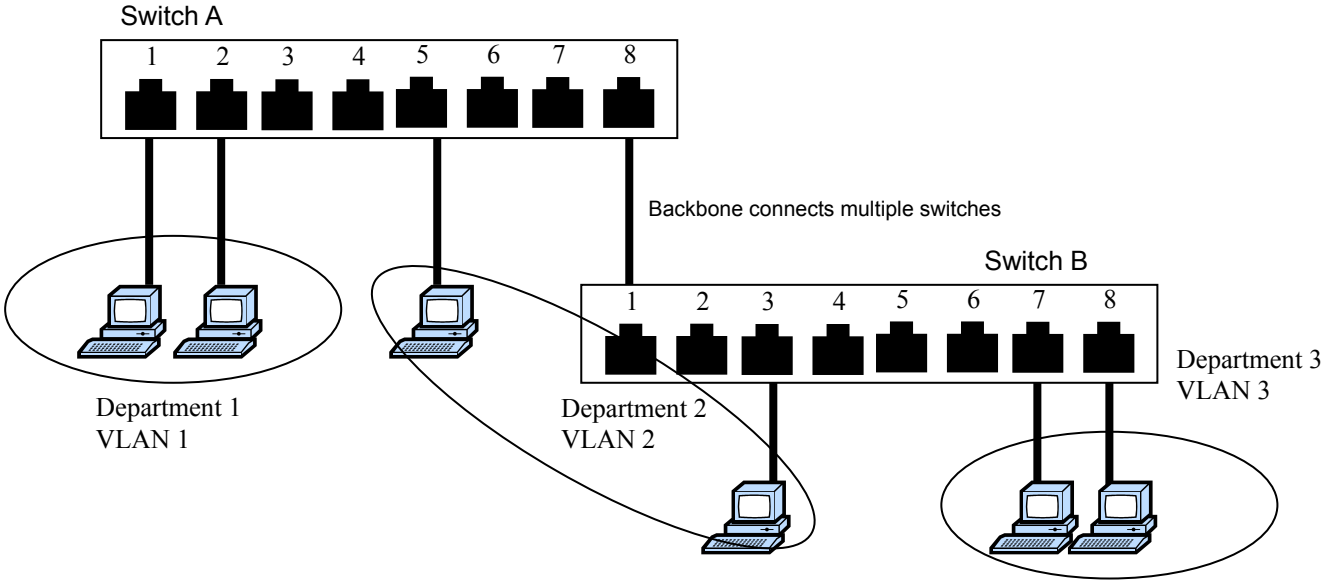
Setting up Virtual LANs (VLANs) on your EDS increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Concept of Virtual LAN (VLAN)

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. As an example, with VLANs you can segment your network according to:

- **Departmental groups**—For example, you can have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups**—For example, you can have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—For example, you can have one VLAN for e-mail users, and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each end-station must be updated manually. With a VLAN setup, if an end-station on VLAN *Marketing* for example is moved to a port in another part of the network, and retains its original subnet membership, you only need to

specify that the new port is on VLAN *Marketin*g. You do not need to carry out any re-cabling.

- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN *Marketing* needs to communicate with devices on VLAN *Financ*e, the traffic must pass through a routing device or Layer 3 Switch.
- **VLANs help to control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices whether they require it or not. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and MOXA EtherDevice Switch

Your EDS provides support for VLANs using the IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 allows each port on your EDS to be placed in:

- Any one VLAN defined on the EDS.
- Several VLANs at the same time using 802.1Q tagging.

The standard requires that you define the *802.1Q VLAN ID* about each VLAN on your EDS before the Switch can use it to forward traffic:

The Management VLAN

A new or initialized EDS contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed in this VLAN, and it is the only VLAN that allows you to access the management software of the EDS over the network.

Communication Between VLANs

If the devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

Your EDS supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Quite simply, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

Typically end-stations (for example, clients) will be untagged members of one VLAN, defined as "Access Port" in EDS, while inter-Switch connections will be tagged members of all VLANs, defined as "Trunk Port" in EDS.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a *tagged* frame.

To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be

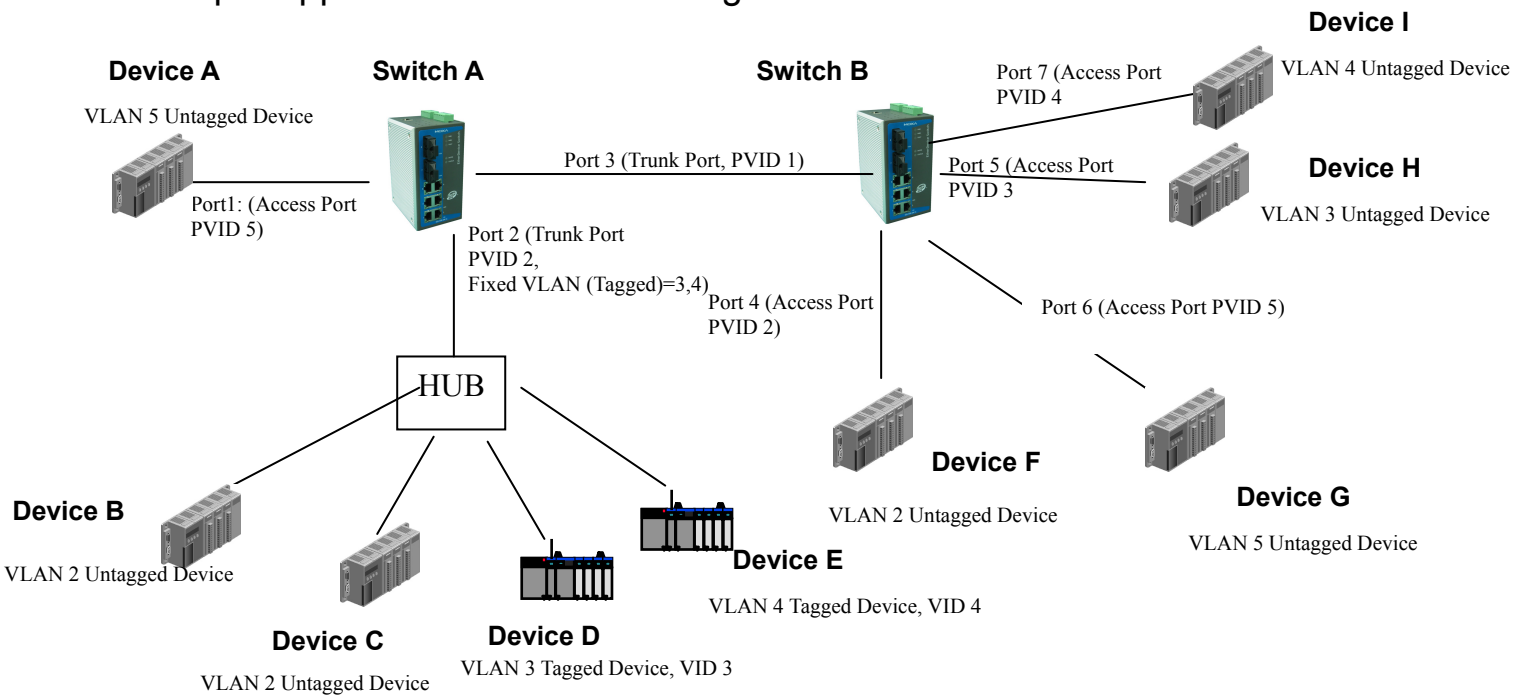
tagged with a VLAN identifier so that the Switches can identify which packets belong in which VLANs. To communicate between VLANs a router must be used.

MOXA EtherDevice Switch supports two types of VLAN port setting for your convenient setting about tagged and untagged configurations.

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port will egress to another Trunk Port (the port needs all packets to carry tag information), EDS will insert this PVID into this packet to help the next 802.1Q VLAN switch recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices/tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigning the port default PVID as its VID.

The following section illustrates how to use these ports to set different applications.

Sample Applications of VLANs using MOXA EtherDevice Switch



In this application,

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as "Trunk Port" with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port can only belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as "Trunk Port." They will use GVRP protocol through the Trunk Port.

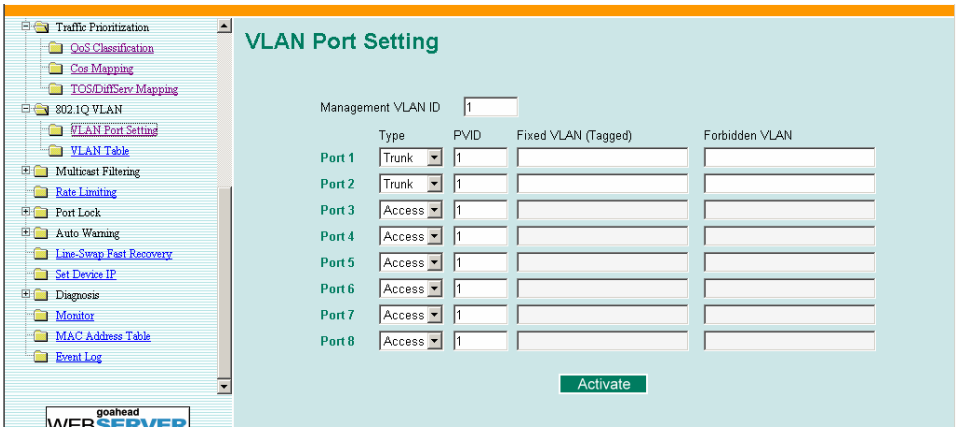
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as "Access Port" with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as "Access Port" with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as "Access Port" with PVID 4.

After proper configuration:

- Packets from device A will travel through "Trunk Port 3" with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by device G, and vice versa.
- Packets from device B and C will travel through "Trunk Port 3" with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4 , and then removes tags received successfully by device F, and vice versa.
- Packets from device D will travel through "Trunk Port 3" with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by device H. Packets from device H will travel through "Trunk Port 3" with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device D.
- Packets from device E will travel through "Trunk Port 3" with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by device I. Packets from device I will travel through "Trunk Port 3" with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device E.

Configuring 802.1Q VLAN

VLAN Port Settings



To configure EDS VLANs, use the VLAN Port Setting page to configure the ports.

Port Type

Setting	Description	Factory Default
Access	This port type is used to connect single devices without tag.	Access
Trunk	Select "Trunk" port type to connect another 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	

ATTENTION

For communication redundancy in the VLAN environment, set "Redundant Port," "Coupling Port," and "Coupling Control Port" as "Trunk Port," since these ports act as the "backbone" to transmit all packets of different VLANs to different EDSs.

Management VLAN Setting

Setting	Description	Factory Default
VID range from 1 to 4094	Set the management VLAN of this EDS-508.	1

Port PVID

Setting	Description	Factory Default
VID range from 1 to 4094	Set the port default VLAN ID for untagged devices that connect to the port.	1

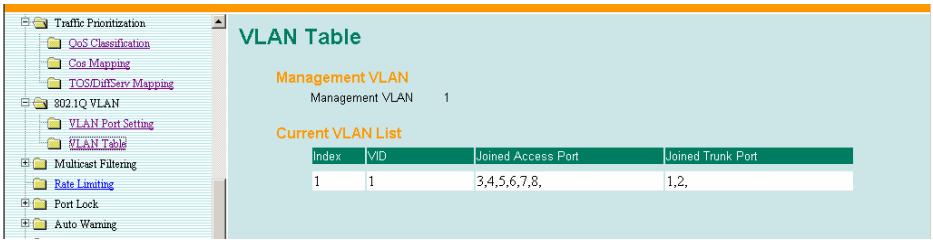
Port Fixed VLAN List (Tagged)

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the other VLAN ID for tagged devices that connect to the "Trunk" port. Use commas to separate different VIDs.	None

Port Forbidden VLAN List

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the VLAN IDs that will not be supported by this trunk port. Use commas to separate different VIDs.	None

VLAN Table



In this table, you can review the created VLAN groups, Joined Access Ports, and Trunk Ports.

NOTE The entire physical connected network system can have a maximum of 64 VLANs settings.

Using Multicast Filtering

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your EDS.

The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet that is intended for "one-to-many" and "many-to-many" communication. Users explicitly request to participate in the communication by joining an end-station to a specific multicast group. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations in a LAN, or VLAN, that belong to the relevant multicast group. Multicast group members can be distributed across multiple subnetworks; thus, multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. It is only at these points that multicast packets are replicated and forwarded, making more efficient use of network bandwidth. A multicast packet is identified by the presence of a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are that it:

- Enables the simultaneous delivery of information to many receivers in the most efficient, logical way.
- Reduces the load on the source (for example, a server) because it does not need to produce multiple copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number of participants or collaborators expands.
- Works with other IP protocols and services, such as Quality of Service (QoS).

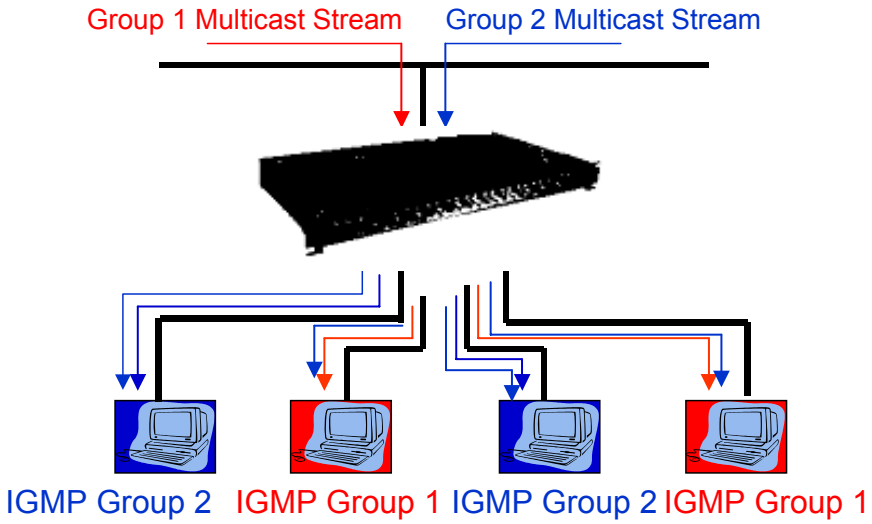
There are situations where a multicast approach is more logical and efficient than a unicast approach. A typical use of multicasts is in video-conferencing, where high volumes of traffic need to be sent to several end-stations simultaneously, but where broadcasting that traffic to all end-stations would seriously reduce network performance. Besides, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use the multicast approach. These industrial Ethernet protocols use

publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require the traffic, thus reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

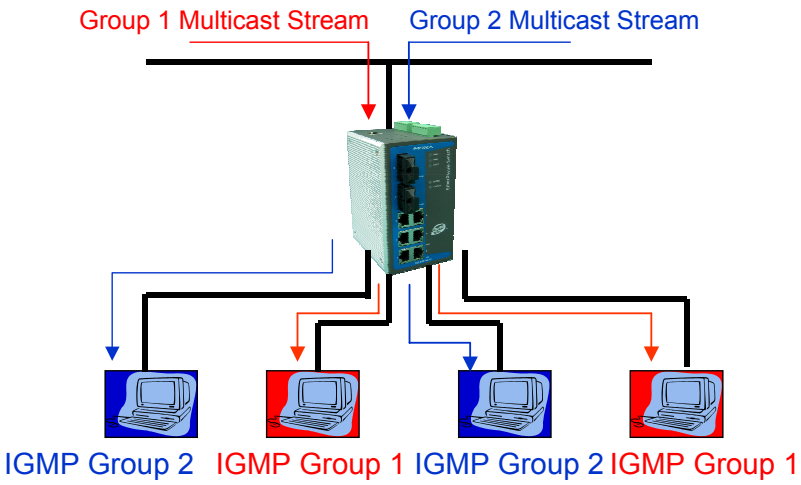
Multicast filtering is the process that ensures that end-stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following figure shows how a network behaves without multicast filtering, and with multicast filtering.

The Network without multicast filtering



All end-stations must handle the traffic whether they need it or not.

The Network with multicast filtering



End-stations only receive dedicated traffic belonging to the same group.

Multicast Filtering and MOXA EtherDevice Switch

Your Switch uses IGMP (Internet Group Management Protocol) Snooping to provide support for automatic multicast filtering. It also supports IGMP query mode.

Snooping Mode

Snooping Mode allows your Switch to forward multicast packets only to the appropriate ports. The Switch "snoops" on exchanges between end-stations and an IGMP device, typically a router, to find those ports that would like to join a multicast group, and then sets its filters accordingly.

Query Mode

Query mode allows the Switch to function as the Querier if it has the lowest IP address in the subnetwork to which it belongs. IGMP querying is enabled by default on the EDS. This helps prevent interoperability issues with some multicast routers that may not follow the lowest IP address election method. Enable query mode if you wish to run multicast sessions on a network that does not contain any IGMP routers (or queriers).

NOTE EDS is compatible with any device that conforms to the IGMP v2 and IGMP v3 protocol.

IGMP Multicast Filtering

IGMP is the system that all IP-supporting network devices use to register end-stations with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. It works as follows:

1. The IP router (or querier) periodically sends *query* packets to all the end-stations in the LANs or VLANs that are connected to it. If your network has more than one IP router, then the one with the lowest IP address becomes the querier. The Switch can be the IGMP querier and will become so if its own IP address is lower than that of any other IGMP queriers connected to the LAN or VLAN.
2. When an IP end-station receives a query packet, it sends a *report* packet back that identifies the multicast group that the end-station would like to join.
3. When the report packet arrives at a port on a Switch with *IGMP Snooping* enabled, the Switch learns that the port is to forward traffic for the multicast group and then forwards the packet to the router.
4. When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
5. When the router forwards traffic for the multicast group to the LAN or VLAN, the Switch units only forward the traffic to ports that received a report packet.

Enabling IGMP Snooping

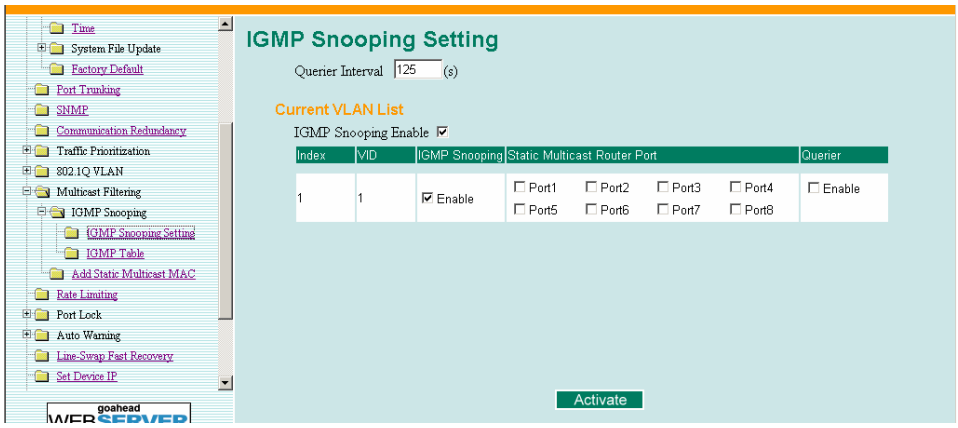
You can enable or disable IGMP Snooping and IGMP querying using the serial console or the Web interface. If IGMP Snooping is not enabled then IP multicast traffic is always forwarded. That is, it floods the network.

Configuring Multicast Filtering

IGMP (Internet Group Management Protocol) is important in industrial networking, and may be used with some field bus protocols over Ethernet such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet). These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could

flood a network with heavy traffic. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.

IGMP Snooping Settings



Querier interval

Setting	Description	Factory Default
User adjustable number	Set the query interval of Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

IGMP Snooping Enable (Global)

Setting	Description	Factory Default
Enable/Disable	Check-mark the check box to enable the IGMP Snooping function globally.	Disabled

IGMP Snooping Enable (per VLAN)

Setting	Description	Factory Default
Enable/Disable	Check-mark the check box to enable the IGMP Snooping function per VLAN.	Enabled if IGMP Snooping Enabled Globally

Static Multicast Router Port

Setting	Description	Factory Default
Select/Deselect	Check-mark the check box to select which ports are connecting to the multicast routers. It's active only when IGMP Snooping is enabled.	Disable

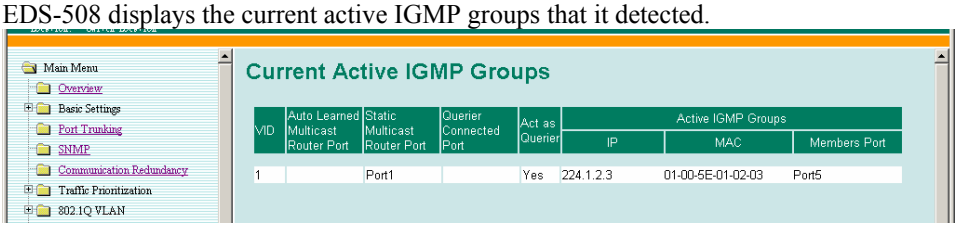
Act as Querier

Setting	Description	Factory Default
Enable/Disable	Check-mark the check box to enable the querier function of EDS-508.	Enabled if IGMP Snooping is Enabled Globally

NOTE At least one switch must be designated the querier when enabling Turbo Ring and IGMP snooping simultaneously.

IGMP Table

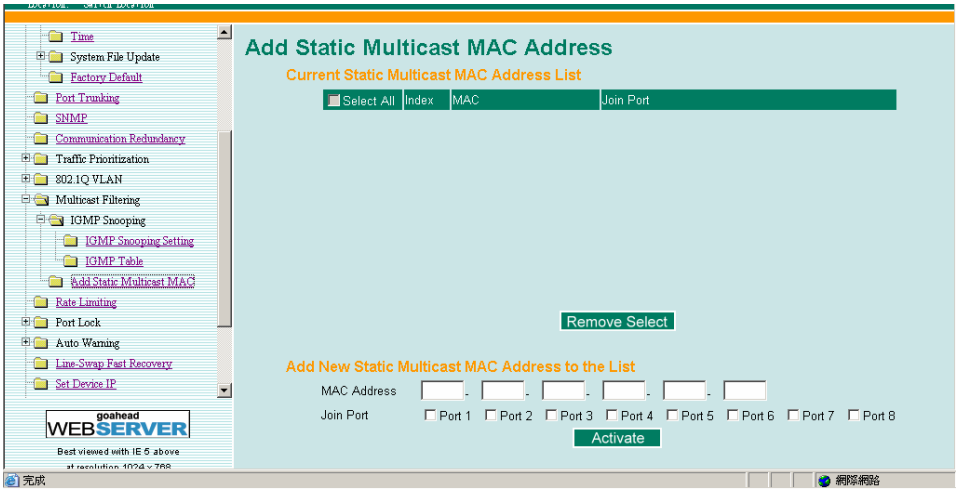
EDS-508 displays the current active IGMP groups that it detected.



The information includes VID, Auto-learned Multicast Router Port, Static Multicast Router Port, Querier Connected Port, and the IP and MAC addresses of active IGMP groups.

Add Static Multicast MAC

MOXA EtherDevice Switch can also support adding multicast groups manually if required.



Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the desired multicast MAC address.	None

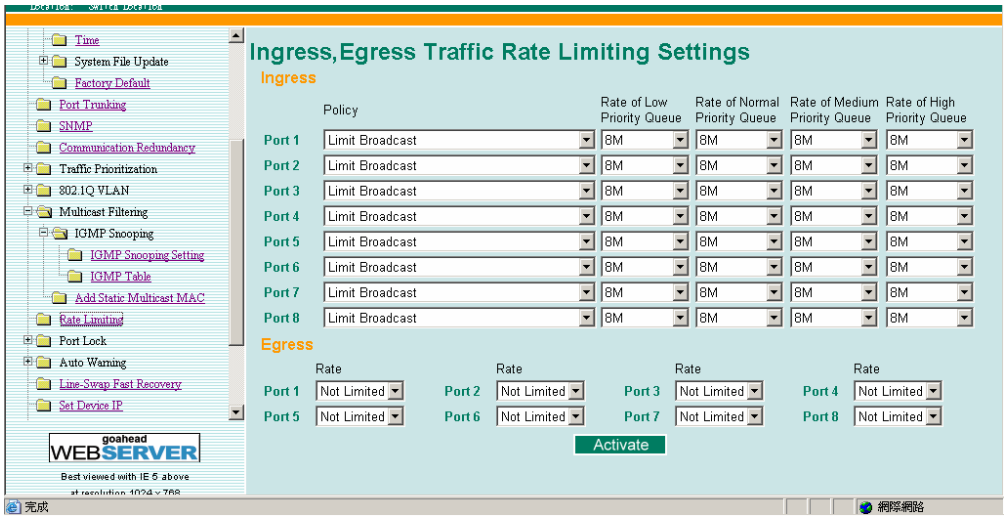
Join Ports

Setting	Description	Factory Default
Select/Deselected	Select the join ports of this multicast group.	None

Using Rate Limiting

Single devices should not occupy unlimited bandwidth, especially when the device malfunctions. The most well-know problem is the broadcast storm caused by an incorrect topology or malfunctioning device. The EDS-508 series not only prevents broadcast storms, but can also configure the ingress/egress rate of unicast/multicast/broadcast packets, thus helping the administrator control fully the limited bandwidth, and prevent unpredictable faults before they occur.

Configuring Rate Limiting



Ingress Policy

Setting	Description	Factory Default
Limit All	Selecting this option prohibits all traffic of broadcast, multicast, unicast packets that exceed the rate set in the following "Rate" field.	Limit Broadcast
Limit Broadcast	Selecting this option prohibits all traffic of broadcast packets that exceed the rate set in the following "Rate" field.	
Limit Broadcast and Multicast	Selecting this option prohibits all traffic of broadcast and multicast packets that exceed the rate set in the following "Rate" field.	
Limit Broadcast, Multicast, and flooded unicast	Selecting this option prohibits all traffic of broadcast, multicast, and flooded unicast (the new unicast address never learned by the EDS) packets that exceed the rate set in the following "Rate" field.	

Rate of Low Priority Queue

Setting	Description	Factory Default
128K/256K/512K /1M/2M/4M/8M	Set the threshold of traffic of limited packets in EDS's low priority queue.	8M

Rate of Normal Priority Queue

Setting	Description	Factory Default
The same or double rate of low priority queue	Set the threshold of traffic of limited packets in EDS's Normal priority queue.	8M

Rate of Medium Priority Queue

Setting	Description	Factory Default
The same or double rate of Normal priority queue	Set the threshold of traffic of limited packets in EDS's medium priority queue.	8M

Rate of High Priority Queue

Setting	Description	Factory Default
The same or double rate of medium priority queue	Set the threshold of traffic of limited packets in EDS's High priority queue.	8M

NOTE By default, EDS is configured to limit broadcast packets not to exceed 8M to protect against broadcast storms caused by careless usage. Can be adjusted by the user.

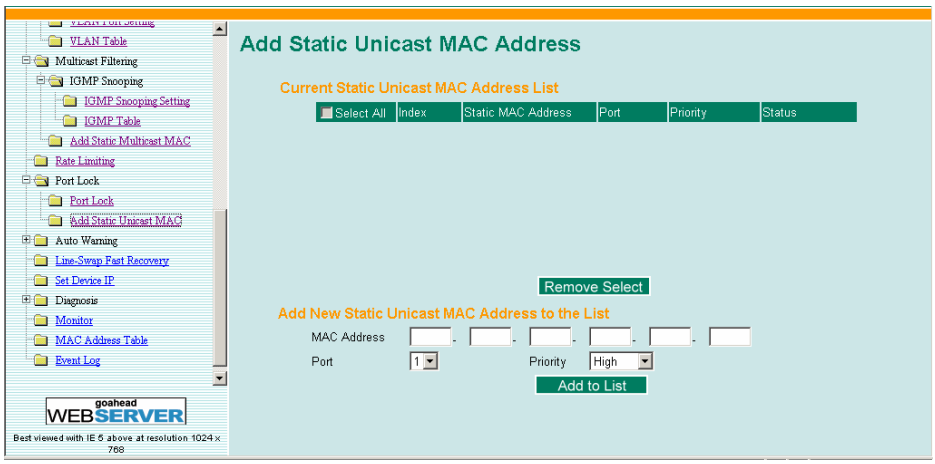
Egress Rate

Setting	Description	Factory Default
No Limit / 128K / 256K / 512K / 1M / 2M / 4M/8M	Set the threshold of EDS's egress packets.	None

Using Port Lock

The EDS-508 series can configure protected static MAC addresses to a specific port. With the Port Lock function, these locked ports will not learn any more addresses, but only allow the traffic coming from preset static MAC addresses, thus helping to block unwanted invasion or careless usage.

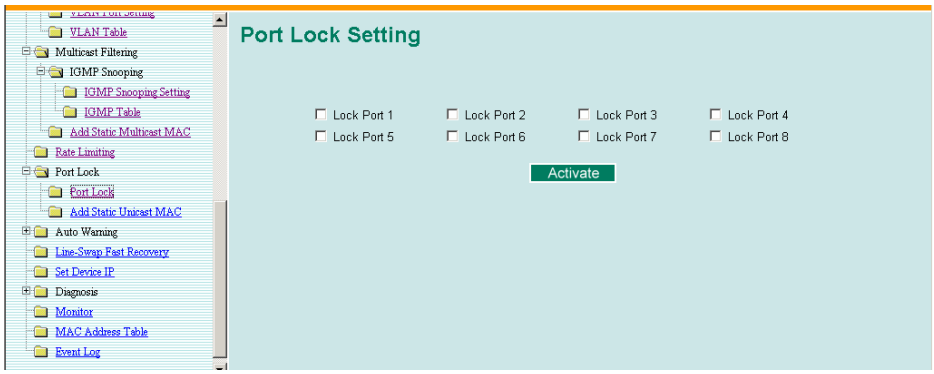
Adding a Static Unicast MAC Address



Add Static Unicast MAC Address

Setting	Description	Factory Default
Unicast MAC Address	Add the static unicast MAC address into the address table.	None
Port	Fix the static address with a dedicated port.	1
Priority	Set the default priority of this static MAC address.	High

Configuring Port Lock



Enabling Port Lock

Setting	Description	Factory Default
Enable/Disable	Check the check box to enable the port lock function.	None

NOTE Before enabling "Port Lock", make sure to add the static unicast MAC address first.

Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, such devices cannot always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. MOXA EtherDevice Switch supports different approaches to warn engineers automatically, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place.

There are three basic steps required to set up the Auto Warning function:

1. **Configuring Email Event Types**
   Select the desired **Event types** from the Console or Web Browser Event type page. (A description of each event type is given later in the *Email Alarm Events setting* subsection.)

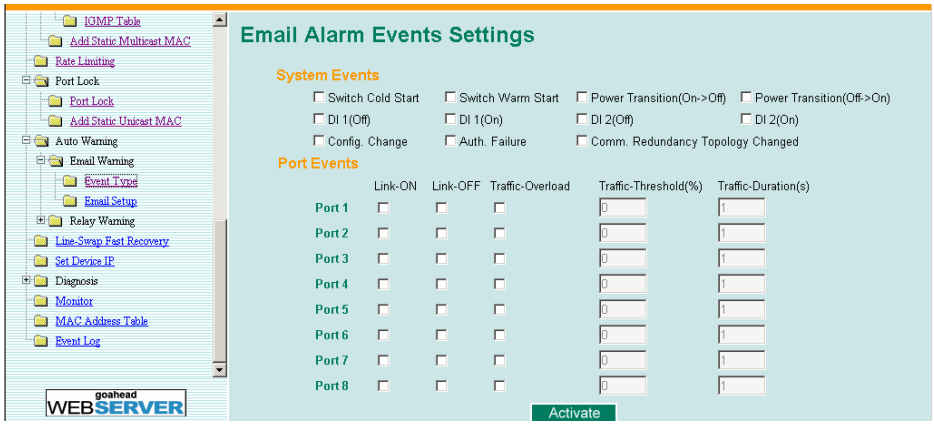
2. **Configuring Email Settings**

   To configure EDS's email setup from the Console interface or browser interface, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address(es) to which warning messages will be sent.

3. **Activate your settings and test email if necessary**

   After configuring and activating your MOXA EtherDevice Switch's Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

Email Alarm Events Settings



Event Types

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the Switch, whereas Port Events are related to the activity of a specific port.

System Event	Warning e-mail is sent when…
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	EDS is rebooted, such as when network parameters are changed (IP address, netmask, etc.).
Power Transition (On→Off)	EDS is powered down.
Power Transition (Off→On)	EDS is powered up.
DI1 (On→Off)	Digital Input 1 is triggered by on to off transition
DI1 (Off→On)	Digital Input 1 is triggered by off to on transition
DI2 (On→Off)	Digital Input 2 is triggered by on to off transition
DI2 (Off→On)	Digital Input 2 is triggered by off to on transition
Configuration Change Activated	Any configuration item is changed.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If Master of Turbo Ring has changed or backup path is activated.
Authentication Failure	An incorrect password is entered.

Port Event	Warning e-mail is sent when…
Link-on	The port is connected to another device.
Link-off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every *Traffic-Duration* seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE The **Traffic-Overload**, **Traffic-Threshold (%)**, and **Traffic-Duration (sec.)** Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

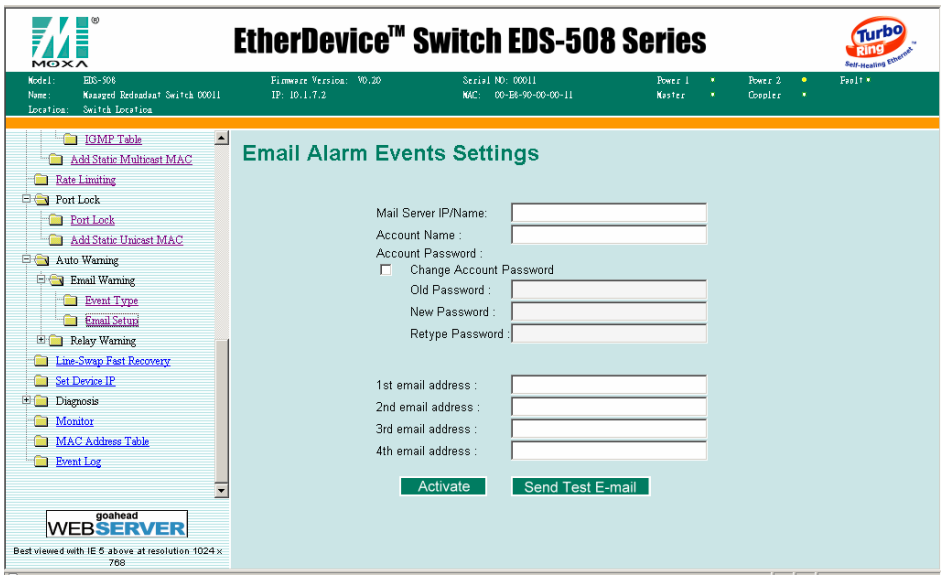
NOTE Warning e-mail messages will have **sender** given in the form:

Moxa_EtherDevice_Switch_0001@Switch_Location

where **Moxa_EtherDevice_Switch** is the default Switch Name, **0001** is EDS's serial number, and **Switch_Location** is the default Server Location.

Refer to the Basic **Settings** section to see how to modify Switch Name and Switch Location.

Email Settings



Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

Account Name

Setting	Description	Factory Default
Max. 45 Charters	Your email account.	None

Password Setting

Setting	Description	Factory Default
Disable/Enable to change Password	To reset the Password from the Web Browser interface, check-mark the Change password check-box, type the Old Password, type the New Password, retype the New password, and then click on Activate.	Disable
Old Password	Type current password when enabled to change password; Max. 45 Characters.	None
New Password	Type new password when enabled to change password.	None
Retype Password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Email Address

Setting	Description	Factory Default
Max. 30 Characters	You can set up to 4 email addresses to receive alarm emails from EDS.	None

Send Test Email

After finishing with the email settings, you should first press the "Activate" button to activate those settings, then press the "Send Test Email" button to verify that the settings are correct.

NOTE Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.
We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without authentication mechanism.

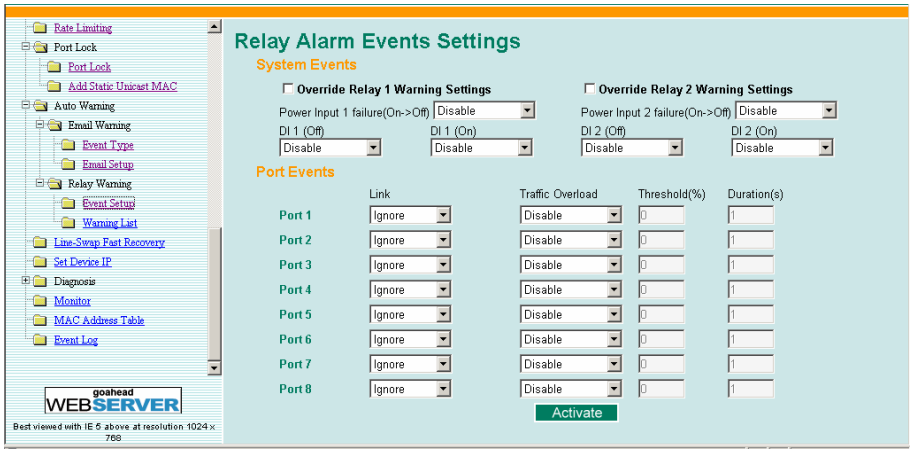
Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are three basic steps required to set up the Relay Warning function:

1. **Configuring Relay Event Types**
   Select the desired **Event types** from the Console or Web Browser Event type page. (A description of each event type is given later in the *Relay Alarm Events setting* subsection.)

2. **Activate your settings**
   After configuring and activating your MOXA EtherDevice Switch's Relay Event Types.

Relay Alarm Events Settings



Event Types

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the Switch, whereas Port Events are related to the activity of a specific port.

MOXA EtherDevice Switch supports two relay outputs. You can configure which relay output is related to which events. This helps administrators identify the importance of the different events.

System Event	Warning Relay output is triggered when…
Power Transition (On→Off)	EDS is powered up.
Power Transition (Off→On)	EDS is powered down.
DI1 (On→Off)	Digital Input 1 is triggered by on to off transition
DI1 (Off→On)	Digital Input 1 is triggered by off to on transition
DI2 (On→Off)	Digital Input 2 is triggered by on to off transition
DI2 (Off→On)	Digital Input 2 is triggered by off to on transition

Port Event	Warning e-mail is sent when…
Link-on	The port is connected to another device.
Link-off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every *Traffic-Duration* seconds if the average Traffic-Threshold is surpassed during that time period.

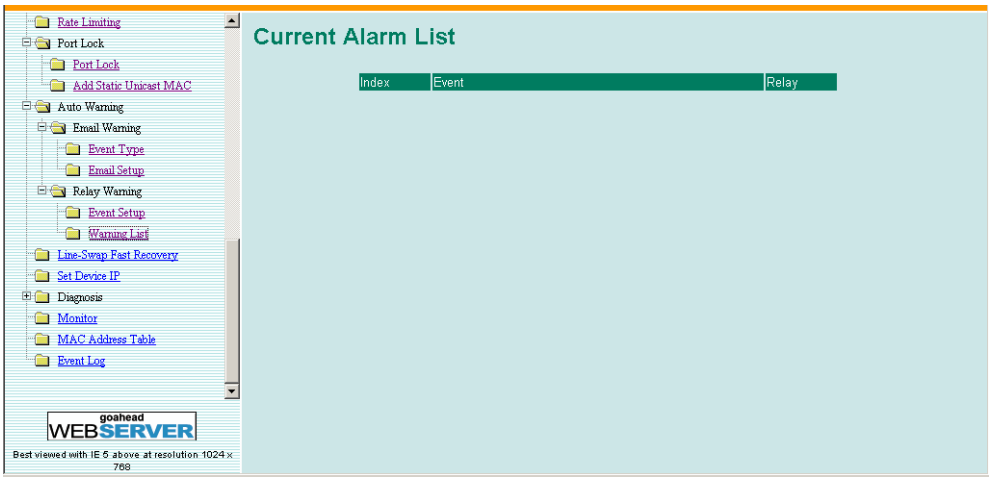
NOTE The **Traffic-Overload**, **Traffic-Threshold (%)**, and **Traffic-Duration (sec)** Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

Override relay alarm settings

Check-mark the check box to override the relay warning setting temporarily. Releasing the relay output will allow administrators until the warning condition has been fixed.

Relay Alarm List

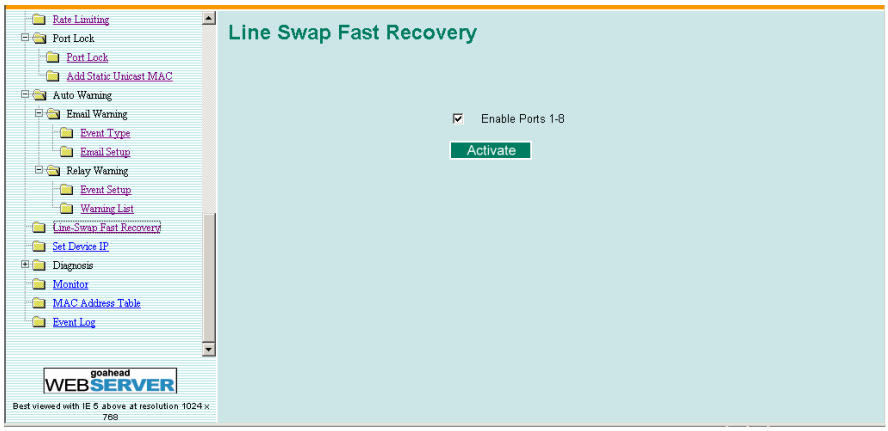
Use this table to see if any relay alarms have occurred.



Using Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows MOXA EtherDevice Switch to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is on the order of a few milliseconds. Compare this with standard commercial switches for which the recovery time could be on the order of several minutes. To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Line-Swap recovery** page, or the Web Browser interface's **Line-Swap fast recovery** page, as shown below.

Configuring Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery

Setting	Description	Factory Default
Enable/Disable	Check-mark the check box to enable the Line-Swap-Fast-Recovery function	Enable

Using Set Device IP

To reduce the effort required to repeatedly set up IP addresses, the EDS-508 series comes equipped with DHCP/BootP server and RARP protocol to automatically set up IP addresses of Ethernet-enabled devices.

When enabled, the **Set device IP** function allows MOXA EtherDevice Switch to automatically assign specific IP addresses to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, MOXA EtherDevice Switch acts as a DHCP server by assigning a connected device with a specific IP address stored in MOXA EtherDevice Switch's internal memory. Each time the connected device is switched on or rebooted, MOXA EtherDevice Switch sends the device the desired IP address.

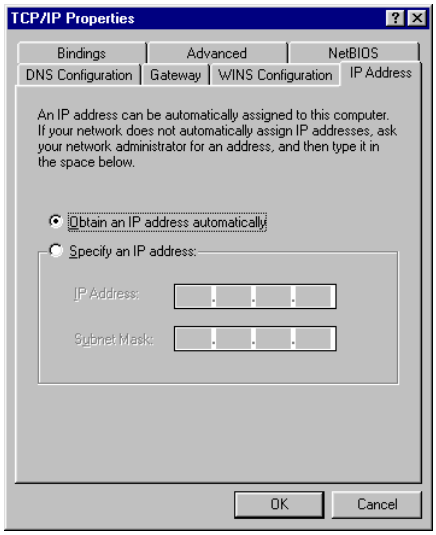
Take the following steps to use the **Set device IP** function:

STEP 1—*set up the connected devices*

Set up the Ethernet-enabled devices connected to MOXA EtherDevice Switch for which you would like the IP addresses to be assigned automatically. The devices must be configured to *obtain* their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to **Obtain an IP address automatically**.

For example, Windows' **TCP/IP Properties** window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

You also need to decide which of MOXA EtherDevice Switch's ports your Ethernet-enabled devices will be connected to. You will need to set up each of these ports separately, as described in the following step.

STEP 2

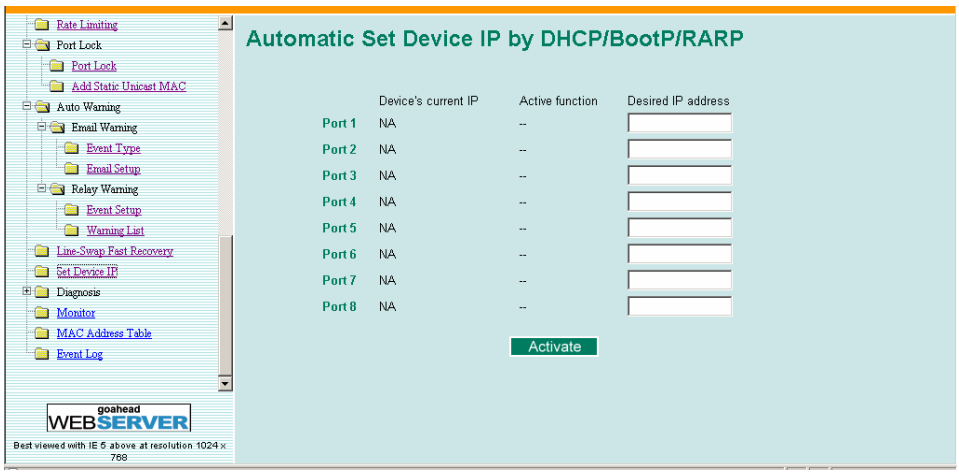
Configure MOXA EtherDevice Switch's **Set device IP** function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that needs to be configured.

STEP 3

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking on the Activate button.
- When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

Configuring Set Device IP



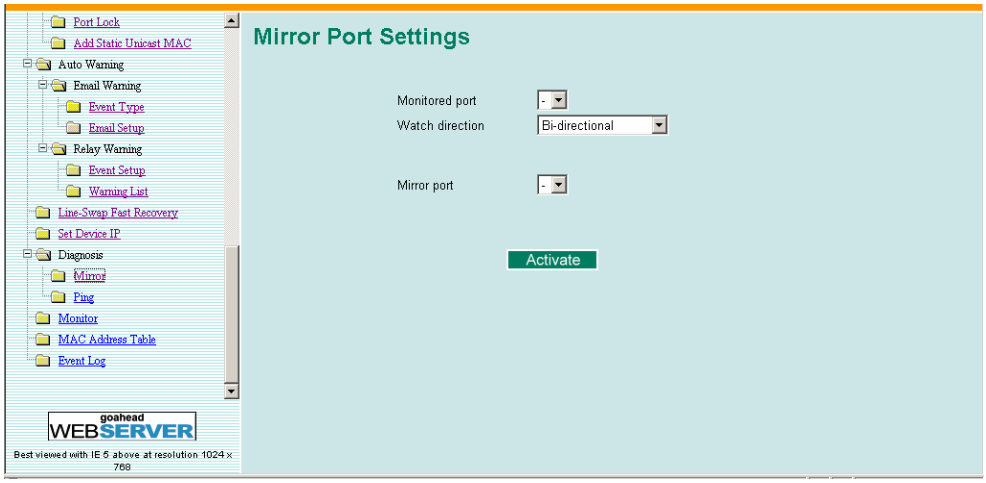
Desired IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

Using Diagnosis

MOXA EtherDevice Switch provides two important tools for administrators to diagnose network systems.

Mirror Port



The **Mirror port** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the *mirror port*) to receive the same data being transmitted to, from, or both to and from, the port under observation. This allows the network administrator to "sniff" the observed port and thus keep tabs on network activity.

Take the following steps to set up the **Mirror Port** function:

STEP 1
Configure MOXA EtherDevice Switch's **Mirror Port** function from either the Console utility or Web Browser interface. You will need to configure three settings:

Monitored Port Select the port number of the port whose network activity will be monitored.

Mirror Port Select the port number of the port that will be used to monitor the activity of the monitored port.

Watch Direction Select one of the following two watch direction options:

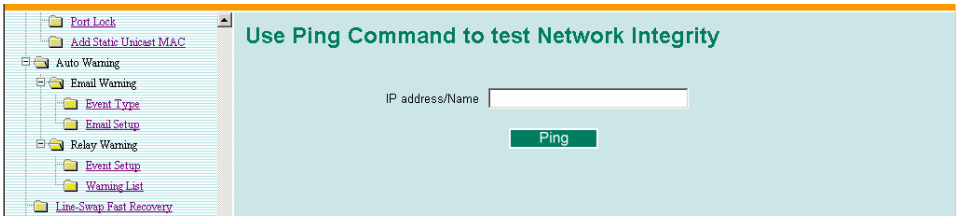
- **Output data stream**
  Select this option to monitor only those data packets being sent *out through* MOXA EtherDevice Switch's port.
- **Bi-directional**
  Select this option to monitor data packets both coming *into*, and being sent *out through*, MOXA EtherDevice Switch's port.

STEP 2

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking on the Activate button.
- When using the Console utility, activate by first highlighting the Activate menu option, and then press **Enter**. You should receive the **Mirror port settings are now active! (Press any key to continue)** message.

Ping



The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from MOXA EtherDevice Switch itself. In this way, the user can essentially "sit on top of MOXA EtherDevice Switch" and send ping commands out through its ports.

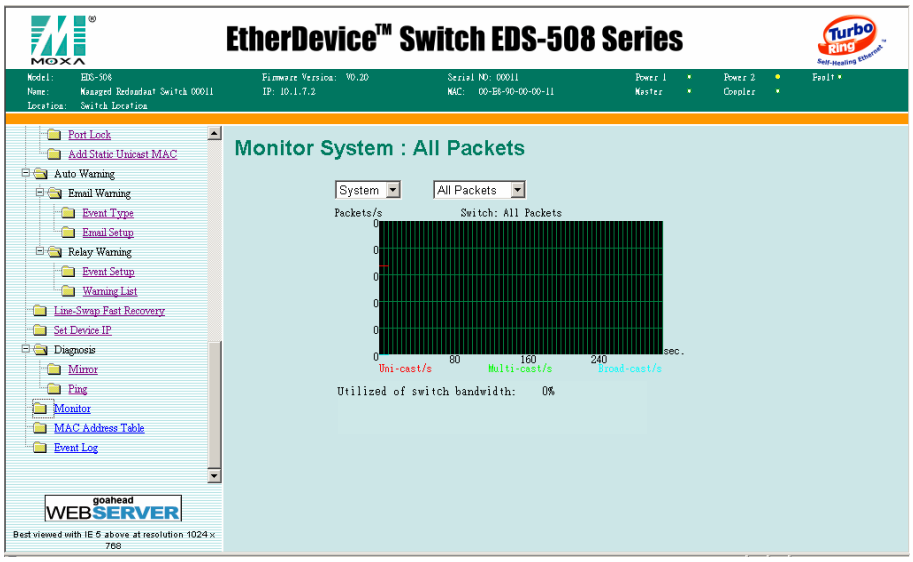
To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click on **Ping** when using the Web Browser interface.

Using Monitor

You can monitor statistics in real time from MOXA EtherDevice Switch's web console and serial console.

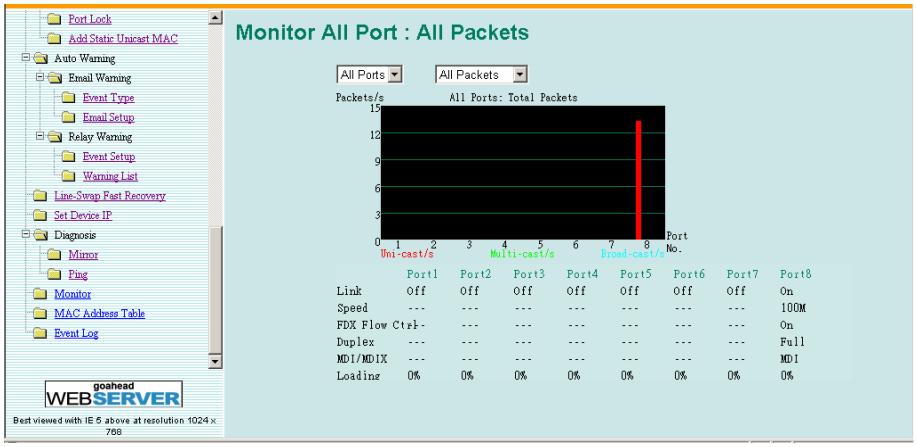
Monitor by Switch

Access the Monitor by selecting "system" from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of MOXA EtherDevice Switch's 8 ports. Click on one of the four options—All Packets, TX Packets, RX Packets, or Error Packets—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from MOXA EtherDevice Switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The All Packets option displays a graph that combines TX, RX, and Error Packet activity. The four graphs (All Packets, TX Packets, RX Packets, and Error Packets) have the same form, so we show here only the All Packets graph. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds). In fact, three curves are displayed on the same graph: **Uni-cast** packets (in red color), **Multi-cast** packets (in green color), and **Broad-cast** packets (in blue color). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



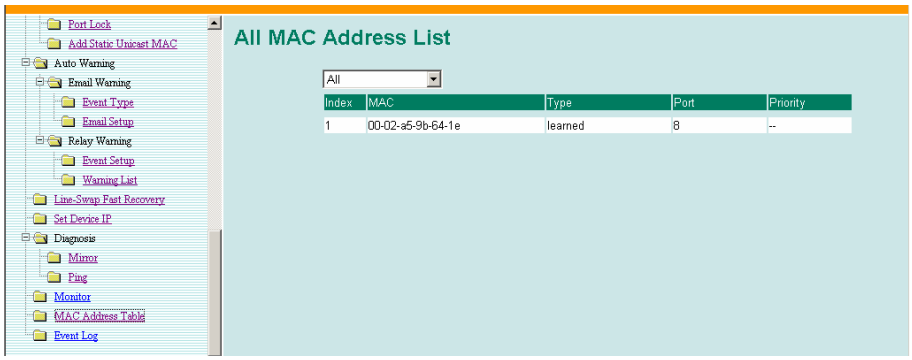
Monitor by Port

Access the Monitor by Port function by selecting the **ALL Port/Port*i***, in which ***i***= 1, 2, …, 8., as shown to the left selection bar. The **Port*i*** options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The red colored bar shows **Uni-cast** packets, the green colored bar shows **Multi-cast** packets, and the blue colored bar shows **Broad-cast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Using the MAC Address Table

This section explains the information provided by MOXA EtherDevice Switch's MAC address table.



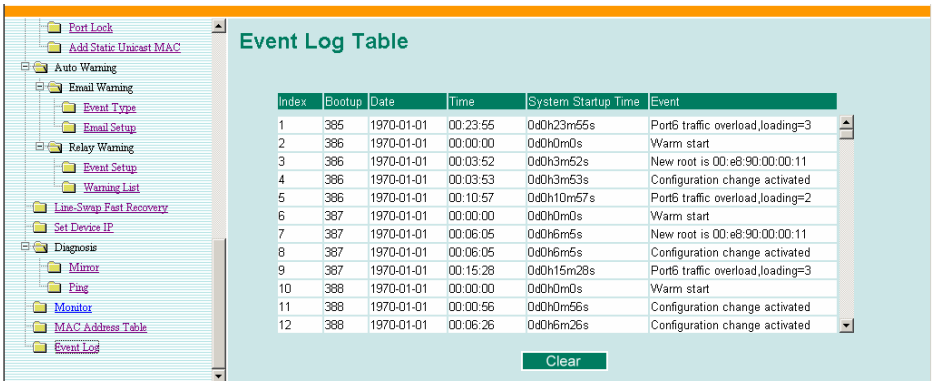
The MAC Address table can be configured to display the following EDS MAC address groups.

ALL	Select this item to show all EDS MAC addresses
ALL Learned	Select this item to show all EDS Learned MAC addresses
ALL Static Lock	Select this item to show all EDS Static Lock MAC addresses
ALL Static	Select this item to show all EDS Static/Static Lock /Static Multicast MAC addresses
ALL Static Multicast	Select this item to show all EDS Static Multicast MAC addresses
Port x	Select this item to show all MAC addresses of dedicated ports

The table will display the following information:

MAC	This field shows the MAC address
Type	This field shows the type of this MAC address
Port	This field shows the port that this MAC address belongs to
Priority	This field shows the priority of this MAC address

Using Event Log


Port Lock
Add Static Unicast MAC
Auto Warning
Email Warning
Event Type
Email Setup
Relay Warning
Event Setup
Warning List
Line-Swap Fast Recovery
Set Device IP
Diagnosis
Mirror
Ping
Monitor
MAC Address Table
Event Log
Event Log Table
Index Bootup Date Time System Startup Time Event
1 385 1970-01-01 00:23:55 0d0h23m55s Port6 traffic overload,loading=3
2 386 1970-01-01 00:00:00 0d0h0m0s Warm start
3 386 1970-01-01 00:03:52 0d0h3m52s New root is 00:e8:90:00:00:11
4 386 1970-01-01 00:03:53 0d0h3m53s Configuration change activated
5 386 1970-01-01 00:10:57 0d0h10m57s Port6 traffic overload,loading=2
6 387 1970-01-01 00:00:00 0d0h0m0s Warm start
7 387 1970-01-01 00:06:05 0d0h6m5s New root is 00:e8:90:00:00:11
8 387 1970-01-01 00:06:05 0d0h6m5s Configuration change activated
9 387 1970-01-01 00:15:28 0d0h15m28s Port6 traffic overload,loading=3
10 388 1970-01-01 00:00:00 0d0h0m0s Warm start
11 388 1970-01-01 00:00:56 0d0h0m56s Configuration change activated
12 388 1970-01-01 00:06:26 0d0h6m26s Configuration change activated
Clear

The following information is displayed in the event table:

Bootup	This field shows how many times the EDS has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the "Basic Setting" page.
Time	The time is updated based on how the current time is set in the "Basic Setting" page.
System Startup Time	The system startup time related to this event.
Events	Events that have occurred.

4

EDS Configurator GUI

EDS Configurator is a comprehensive Windows-based GUI that is used to configure and maintain multiple MOXA EtherDevice Switches. A suite of useful utilities is available to help you locate MOXA EtherDevice Switches attached to the same LAN as the PC host (regardless of whether or not you know the Switches' IP addresses), connect to a MOXA EtherDevice Switch whose IP address is known, modify one or multiple MOXA EtherDevice Switches' network configurations, and update the firmware of one or more MOXA EtherDevice Switches. EDS Configurator is designed to provide you with instantaneous control of *all* of your MOXA EtherDevice Switches, regardless of location. You may download the EDS Configurator software from Moxa's website free of charge.

This chapter includes the following sections:

- **Starting EDS Configurator**
- **Broadcast Search**
- **Search by IP address**
- **Upgrade Firmware**
- **Modify IP Address**
- **Export Configuration**
- **Import Configuration**
- **Unlock Server**

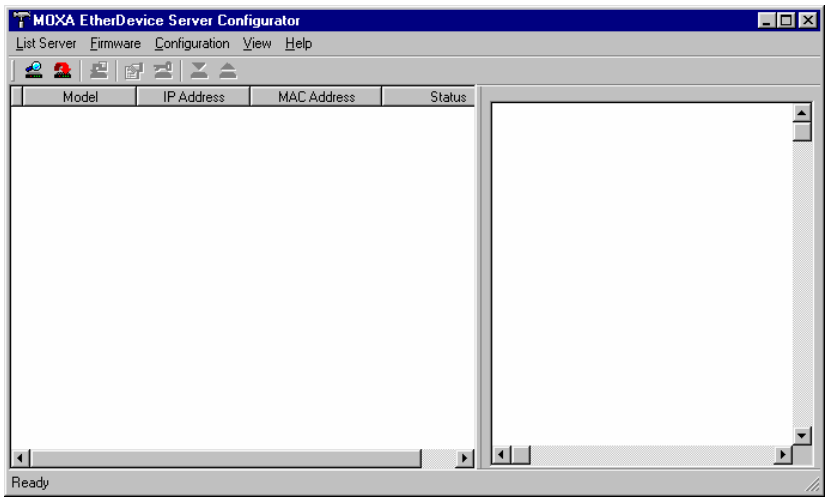
Starting EDS Configurator

To start EDS Configurator, locate and then run the executable file **edscfgui.exe**.

NOTE You may download the EDS Configurator software from Moxa's website at www.moxa.com.

For example, if the file was placed on the Windows desktop, it should appear as follows. Simply double click on the icon to run the program.

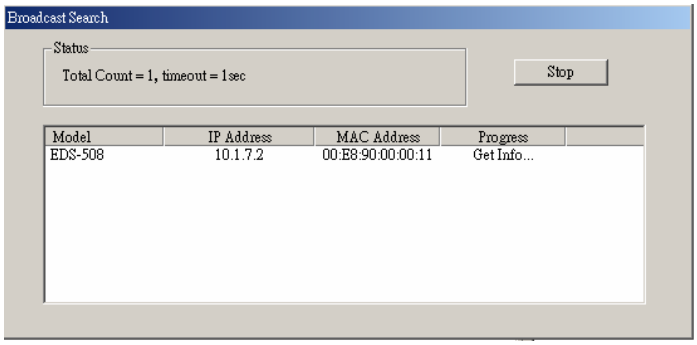
The MOXA EtherDevice Switch Configurator window will open, as shown below.



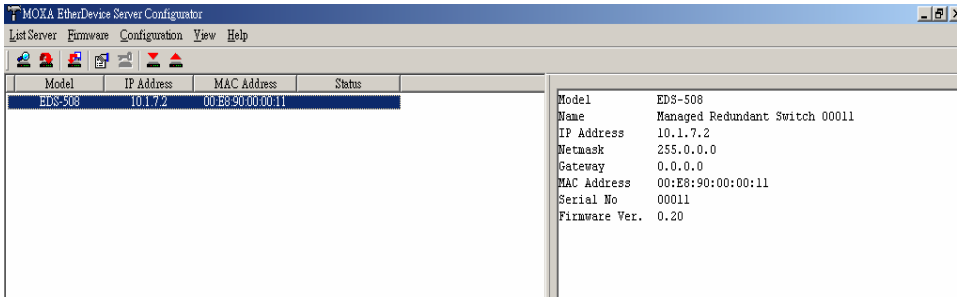
Broadcast Search

Use the Broadcast Search utility to search the LAN for all MOXA EtherDevice Switches that are connected to the LAN. Note that since the search is done by MAC address, Broadcast Search will not be able to locate MOXA EtherDevice Servers connected outside the PC host's LAN. Start by clicking on the Broadcast Search icon , or by selecting **Broadcast Search** under the **List Server** menu.

The Broadcast Search window will open, displaying a list of all Switches located on the network, as well as the progress of the search.



Once the search is complete, the Configurator window will display a list of all Switches that were located.

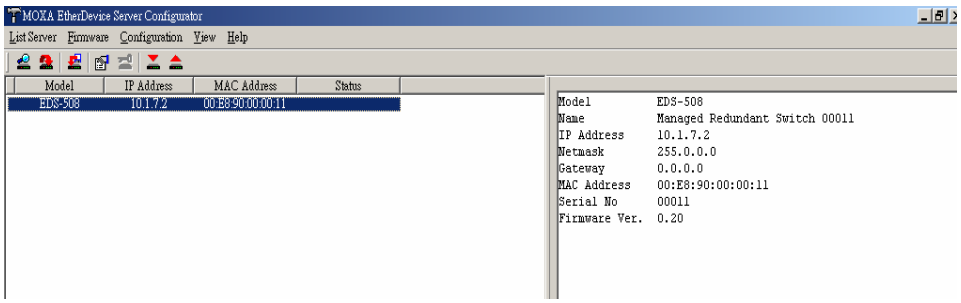


Search by IP address

This utility is used to search for MOXA EtherDevice Switches one at a time. Note that the search is conducted by IP address, so you should be able to locate any MOXA EtherDevice Switch that is properly connected to your LAN, WAN, or even the Internet. Start by clicking on the Specify by IP address icon , or by selecting **Specify IP address** under the **List Server** menu.

The **Search Server with IP Address** window will open. Enter the IP address of the Switch you wish to search for, and then click **OK**.

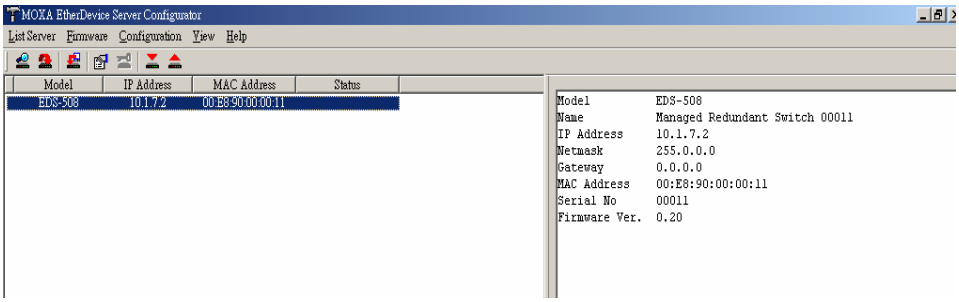
Once the search is complete, the Configurator window will add the Switch to the list of Switches.



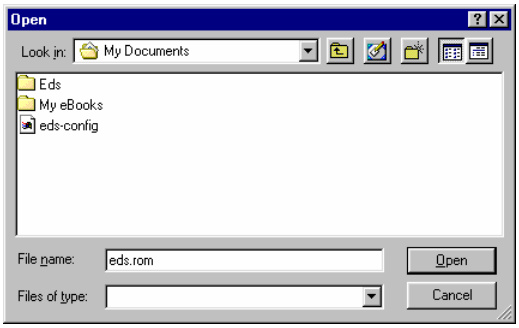
Upgrade Firmware

Keep your MOXA EtherDevice Switch up to date with the latest firmware from Moxa. Take the following steps to upgrade the firmware:

1. Download the updated firmware (*.rom) file from the Moxa website (www.moxa.com).
2. Highlight the switch (from the **MOXA EtherDevice Switch Configurator** window) whose firmware you wish to upgrade.



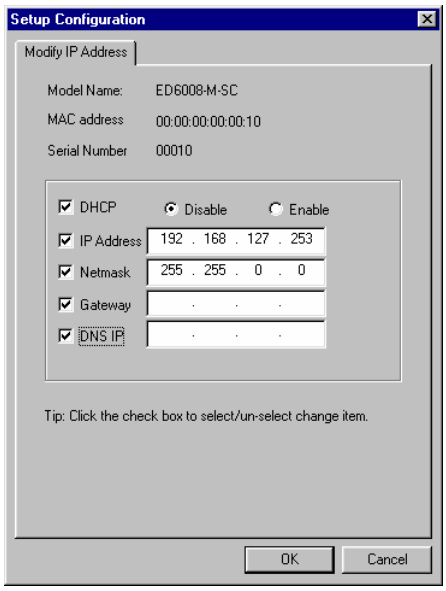
3. Click on the **Upgrade Firmware** toolbar icon , or select **Upgrade** under the **Firmware** menu. If the Switch is Locked, you will be prompted to input the switch's User Name and Password.
4. Use the **Open** window to navigate to the folder that contains the firmware upgrade file, and then click on the correct "*.rom" file (**eds.rom** in the example shown below) to select the file. Click on **Open** to activate the upgrade process.



Modify IP Address

You may use the Modify IP Address function to reconfigure MOXA EtherDevice Switch's network settings. Start by clicking on the Modify IP address icon , or by selecting **Modify IP address** under the **Configuration** menu.

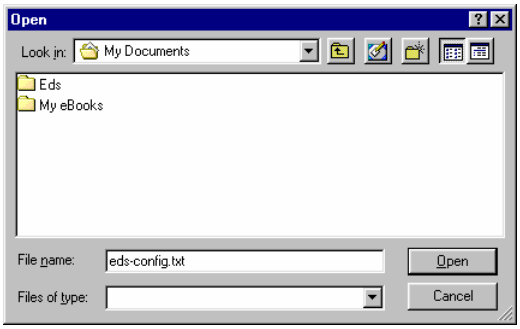
The **Setup Configuration** window will open. Checkmark the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter IP Address, Netmask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.



Export Configuration

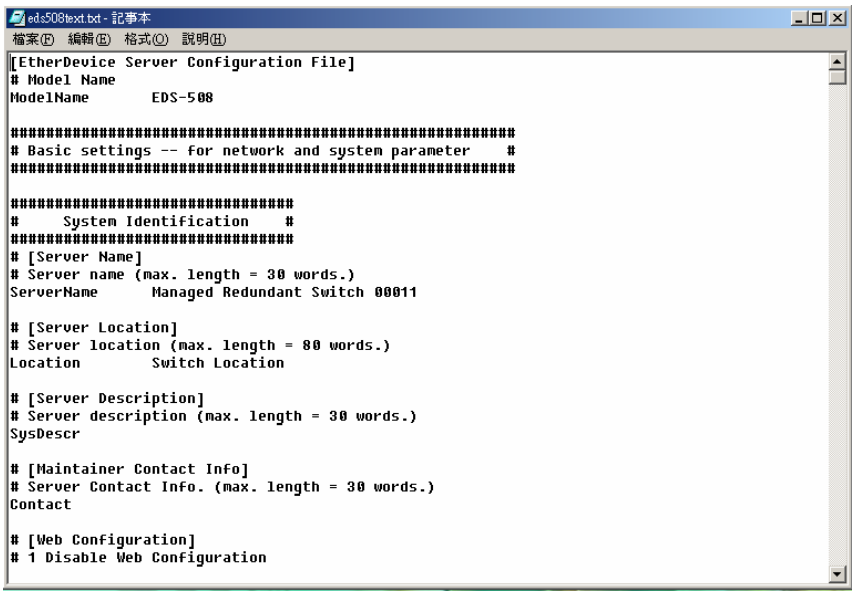
The **Export Configuration** utility is used to save the entire configuration of a particular MOXA EtherDevice Switch to a text file. Take the following steps to export a configuration:

1. Highlight the switch (from the Server list in the Configurator window's left pane), and then click on the **Export** toolbar icon or select **Export Configuration** from the **Configuration** menu. Use the **Open** window to navigate to the folder in which you want to store the configuration, and then type the name of the file in the File name input box. Click on **Open**.



2. Click on **OK** when the **Export configuration to file OK** message appears.

3. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.

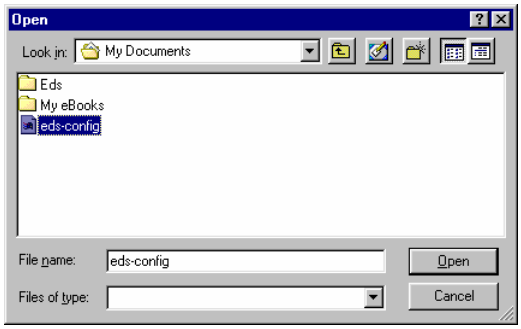


Import Configuration

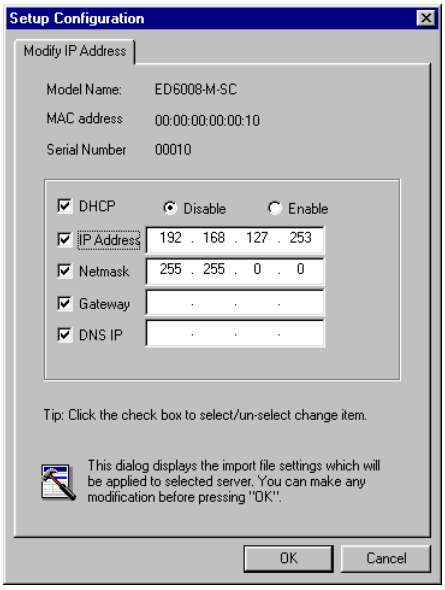
The **Import Configuration** function is used to import an entire configuration from a text file to MOXA EtherDevice Switch. This utility can be used to transfer the configuration from one MOXA EtherDevice Switch to another, by first using the Export Configuration function (described in the previous section) to save a Switch configuration to a file, and then using the Import Configuration function. Take the following steps to import a configuration:

1. Highlight the server (from the MOXA EtherDevice Switch list in the Configurator window's left pane), and then click on the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.

2. Use the **Open** window to navigate to the text file that contains the desired configuration. Once the file is selected, click on **Open** to initiate the import procedure.



3. The **Setup Configuration** window will be displayed, with a special note attached at the bottom. Parameters that have been changed will be activated with a check mark. You may make more changes if necessary, and then click **OK** to accept.


Setup Configuration
Modify IP Address
Model Name: ED6008-M-SC
MAC address 00:00:00:00:00:10
Serial Number 00010
DHCP
Disable
Enable
IP Address 192 . 168 . 127 . 253
Netmask 255 . 255 . 0 . 0
Gateway
DNS IP
Tip: Click the check box to select/un-select change item.
This dialog displays the import file settings which will be applied to selected server. You can make any modification before pressing "OK".
OK
Cancel

4. Click on **Yes** in response to the following warning message to accept the new settings.

MOXA EtherDevice Server Configurator
Warning!
Some or all of your MOXA EtherDevice Server's own network settings have been changed.
Once the new settings have been updated,you may need to use the new network settings (IP address, Netmask, Gateway, etc.) to re-establish a Console session with your MOXA EtherDevice Server. Would you like to update network setting now ?
Yes
No

Unlock Server

The Unlock Server function is used to open a password protected Switch so that the user can modify its configuration, import/export a configuration, etc. To begin with, we point out that there are six possible responses under the **Status** column. The **Status** of a MOXA EtherDevice Switch indicates how the switch was located (by MOXA EtherDevice Switch Configurator), and what type of password protection it has.

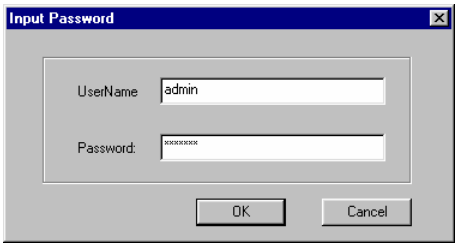
The six options are as follows (note that the term **Fixed** is borrowed from the standard *fixed IP address* networking terminology):

- **Locked**
  The Switch is password protected, "Broadcast Search" was used to locate it, and the password has not yet been entered from within the current Configurator session.
- **Unlocked**
  The Switch is password protected, "Broadcast Search" was used to locate it, and the password has been entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this Switch will not require re-entering the server password.
- **Blank**
  EDS is not password protected, and "Broadcast Search" was used to locate it.

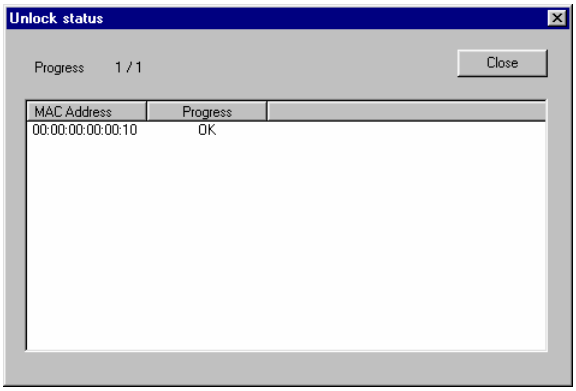
- **Fixed**
  EDS is not password protected, and "Search by IP address" was used to locate it manually.
- **Locked Fixed**
  EDS is password protected, "Search by IP address" was used to locate it manually, and the password has not yet been entered from within the current Configurator session.
- **Unlocked Fixed**
  EDS is password protected, "Search by IP address" was used to locate it manually, and the password has been entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this MOXA EtherDevice Switch will not require re-entering the server password.

Follow the steps given below to unlock a locked MOXA EtherDevice Switch (i.e., a MOXA EtherDevice Switch with Status "Locked" or "Locked Fixed"). Highlight the server (from the MOXA EtherDevice Switch list in the Configurator window's left pane), and then click on the **Unlock** toolbar icon , or select **Unlock** from the **Configuration** menu.

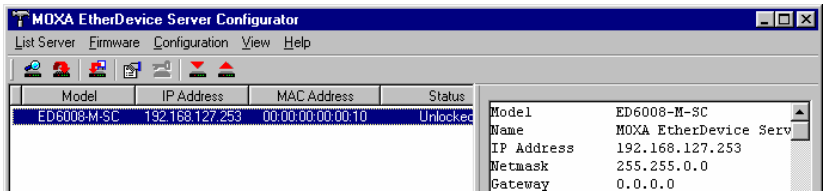
1. Enter the Switch's **User Name** and **Password** when prompted, and then click **OK**.



2. When the **Unlock status** window reports Progress as **OK**, click on the **Close** button in the upper right corner of the window.



3. The Status of the Switch will now read either **Unlocked** or **Unlocked Fixed**.



A

MIB Groups

MOXA EtherDevice Switch comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups that MOXA EDS-508 series supports are:

MIB II.1 – System Group

MIB II.2 – Interfaces Group

MIB II.4 – IP Group

MIB II.5 – ICMP Group

MIB II.6 – TCP Group

MIB II.7 – UDP Group

MIB II.10 – Transmission Group

MIB II.11 – SNMP Group

MIB II.17 – Dot1dBridge Group

MIB II.17.2 – RSTP-MIB Group

MIB II.17.6 – pBridge Group

MIB II.17.7 – qBridge Group

EDS-508 also provides a private MIB file, located in the file “MOXA-EDS508-MIB.my” on the EDS-508 Series utility CD-ROM.

B

Specifications

Technology

Standards	IEEE802.3, 802.3u, 802.3x, 802.1D, 802.1W, 802.1Q, 802.1p
Protocols	IGMP V1/V2/V3 device, GVRP, SNMP V1/V2C/V3, DHCP Server/Client, BootP, TFTP, SNTP, SMTP, RARP and EDS-SNMP OPC server (Optional)
MIB	MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, Q-BRIDGE MIB, Bridge MIB, RSTP MIB
Forwarding and Filtering Rate	148800 pps
Processing Type	Store and Forward
Flow Control	IEEE802.3x, back pressure
Address Table Size	2K uni-cast addresses

Interface

RJ45 Ports	10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection
Fiber Ports	100BaseFX ports (SC connector)
Console	RS-232 (RJ45)
LED Indicators	Power, Faults, 10/100M, Ring Master and Ring Coupler
Alarm Contact	Two relay outputs with current carrying capacity of 1A @ 24 VDC
Digital Input	Two inputs with the same ground, but electrically isolated from the electronics • For state "1": +13 to +30V • For state "0": -30 to +3V • Max. input current: 8 mA

Optical Fiber

	Multi mode	Single mode, 15	Single mode, 40	Single mode, 80
Distance, km	5	15	40	80
Wavelength, nm	1310	1310	1310	1550
Min. TX Output, dBm	-20	-15	-5	-5
Max. TX Output, dBm	-14	-6	0	0
Sensitivity, dBm	-34 to -30	-36 to -32	-36 to -32	-36 to -32
Recommended Diameter,	50/125	9/125	9/125	9/125
Diameter (Core/Cladding), μm	1 dB/km, 800 MHz*km			

Power

Input Voltage	12 to 48 VDC, redundant inputs
Input Current (@24V)	0.29A: (EDS-508) 0.43A: (EDS-508-MM-SC, EDS-508-SS-SC)
Connection	Two removable 6-pin terminal blocks
Overload Current Protection	Present, can withstand 1.6A
Reverse Polarity Protection	Present

Mechanical

Casing	IP30 protection, aluminum case
Dimensions	80.5 x 135 x 105 mm (W x H x D)
Weight	1.04 kg
Installation	DIN-Rail, Wall Mounting (optional kit)
Casing	IP30 protection, aluminum case

Environment

Operating Temperature	0 to 60°C (32 to 140°F) -40 to 75°C (for "-T" models)
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5% to 95% (non-condensing)

Regulatory Approvals

Safety	UL60950, UL 508, CSA C22.2 No. 60950, EN60950(E212360)
Hazardous Location	UL/cUL Class I, Division 2, Groups A, B, C and D (E238559). ATEX Class I, Zone 2, EEx nC IIC (03CA24537)
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), Level 3 EN61000-4-3 (RS), Level 3 EN61000-4-4 (EFT), Level 3 EN61000-4-5 (Surge), Level 3 EN61000-4-6 (CS), Level 3
Shock	IEC60068-2-27
Freefall	IEC60068-2-32
Vibration	IEC60068-2-6
MTBF	260,000 hours
WARRANTY	5 years

C

Service Information

This appendix shows you how to contact Moxa for information about this and other products, and how to report problems.

In this appendix, we cover the following topics.

- **MOXA Internet Services**
- **Problem Report Form**
- **Product Return Procedure**

MOXA Internet Services

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Moxa Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

E-mail for technical support.....support@moxanet.com

World Wide Web (WWW) Site for product information:

.....http://www.moxa.com

Problem Report Form

MOXA EDS-508 Series

Customer name:	
Company:	
Tel:	**Fax:**
Email:	**Date:**

1. Moxa Product: ☐ EDS-508 ☐ EDS-508-MM-SC ☐ EDS-508-SS-SC
☐EDS-508-SS-SC-80 ☐EDS-508-T ☐EDS-508-MM-SC-T
☐EDS-508-SS-SC-T ☐EDS-508-SS-SC-80-T

2. Serial Number: _____

Problem Description: Please describe the symptoms of the problem as clearly as possible, including any error messages you see. A clearly written description of the problem will allow us to reproduce the symptoms, and expedite the repair of your product.

Product Return Procedure

For product repair, exchange, or refund, the customer must:

- Provide evidence of original purchase.
- Obtain a Product Return Agreement (PRA) from the sales representative or dealer.
- Fill out the Problem Report Form (PRF). Include as much detail as possible for a shorter product repair time.
- Carefully pack the product in an anti-static package, and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package, and include a description of the problem, along with the return address and telephone number of a technical contact.